

EXHIBIT 10

Messages

Received from Malia Zimmerman on Apr 13, 2017 6:50:52 PM

MZ

CIA's Pompeo rips WikiLeaks as 'hostile intelligence service' abetted by Russia <http://www.foxnews.com/politics/2017/04/13/cias-pompeo-rips-wikileaks-as-hostile-intelligence-service-abetted-by-russia.html>

Received from Malia Zimmerman on Apr 13, 2017 6:51:11 PM

MZ

Good time for us to Contact Wikileaks

Received from Malia Zimmerman on Apr 14, 2017 8:27:14 PM

MZ

This is from WikiLeaks. This is the email chain for the Hillary Clinton campaign team. They were passing around scandalous information about Bernie Sanders. If any of them worked for the White House and are cleared for classified information then they a possible suspect as being a leaker

Received from Malia Zimmerman on May 10, 2017 1:01:32 PM

MZ

Hi Adam, can you ask your new sources about Seth rich - specifically if they know for sure that he sent emails to WikiLeaks and if so how they know that.
Secondarily
Any other information you can get on selling the information to WikiLeaks, or the hacking group, would be very helpful.
We also would like to know if the FBI got involved with the case or any other agency? Or is it just the DC police?
Thanks

Received from Malia Zimmerman on May 16, 2017 9:32:58 AM

MZ

Wikileaks retweeted our story. Up to 207k tweets about it

Received from Malia Zimmerman on May 16, 2017 4:13:07 PM

MZ

Rod you could mention that Wikileaks retweeted the story

Received from Clare Lopez on May 16, 2017 4:19:48 PM

CL

Why does Seth's family deny his connection to Wikileaks & how would they know anyway?

Received from Malia Zimmerman on May 16, 2017 8:28:26 PM

MZ

<http://money.cnn.com/2017/05/16/media/seth-rich-family-response-claims-of-wikileaks-contact/index.html>

Received from Malia Zimmerman on May 16, 2017 10:38:43 PM

MZ

http://okcfox.com/news/nation-world/no-facts-no-evidence-supporting-claim-slain-dnc-staffer-tied-to-wikileaks-family-says?utm_content=buffer19dd4&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

Received from Malia Zimmerman on May 16, 2017 10:38:44 PM

MZ

Wikileaks calls this the most comprehensive report yet on Seth rich. Im not sure about that

Received from Malia Zimmerman on May 19, 2017 2:01:47 PM

MZ

Adam do you think Wikileaks will say whether they made a payment to Seth Rich by either bitcoin or other means but not say why? The NSA guy said he's tracing a bitcoin payment to Seth rich from Wikileaks.

Sent to Rod Wheeler on May 19, 2017 9:27:54 PM

Gentlemen
I have contacted some Marines who are now FBI SA's they said it was the Technical branch who work with D.C. Police so they are hunting them down for info.
We tracked down a bridge chain looking for a payment of some kind from Wikileaks, but that one was a dry hole. So we are looking for others to track down.
Will touch base tomorrow.

Sent to Adam Housley, Malia Zimmerman on May 19, 2017 9:29:31 PM

Gentlemen
I have contacted some Marines who are now FBI SA's they said it was the Technical branch who work with D.C. Police so they are hunting them down for info.
We tracked down a bridge chain looking for a payment of some kind from Wikileaks, but that one was a dry hole. So we are looking for others to track down.
Will touch base tomorrow.

Messages



Received from Matthew Boyle on May 21, 2017 1:34:46 PM

<http://bigleaguepolitics.com/kim-dotcom-offers-congress-evidence-prove-seth-rich-wikileaks-source/>

Received from maliamzimmerman@icloud.com on May 22, 2017 11:40:28 AM

Ms. Zimmerman,

My name is Matt Taibbi. I'm a reporter for Rolling Stone.

Had a question I wanted to ask you - and please don't worry, it would be off the record. I'm writing because I heard something very similar to what you reported about Seth Rich. I heard it months ago, and was unable to confirm it (enough to report anyway). I've been skeptical of a lot of the Russia-Trump hysteria and though I don't necessarily believe Rich was the Wikileaks source, there are at least enough unknowns with that case to make it hard to dismiss.

I'm curious about your federal investigator source. Did you speak with that person? Do you stand by that part of the story? Is there any chance that he/she could characterize some of those Wikileaks emails?

Again, I'm not writing about this (not now, anyway). I'm just curious and though I've seen many outraged pieces purporting to debunk your report, I haven't seen anyone address the issue of your federal source. Are you going to publish more on that? There's no retraction coming, right? I just want to make sure that part of your story is still unchanged.

Thank you,
Matt Taibbi
917-723-6798



Received from maliamzimmerman@icloud.com on May 22, 2017 4:29:30 PM

this is what we told them before on May 16 perAdam Adam gave me three sources in the NSA, NSC and CIA who confirmed the Wikileaks-Seth Rich connection.

The one who we have the most info from is in the guy in NSA. He actually saw the emails. During his service, he has been honored multiple times by his agency, is known for being an intel whiz and is very high up in his department. He is trying to get us some of the documents.



Received from maliamzimmerman@icloud.com on May 22, 2017 6:25:03 PM

Rod Wheeler, former DC homicide detective

Ed Butowsky put former DC homicide detective Rod Wheeler in touch with Seth Rich's father, Joel Rich. During the first call in March when they connected, Joel's wife Mary and his son Aaron, Seth's brother, were on the call.

Joel Rich asked Ed to hire Rod Wheeler on the family's behalf, because he said he liked Rod and was familiar with him being on television for Fox News, where he was a Fox News contributor. They understood if there were any fees, Ed Butowsky would take care of those. Ed also made a donation to Seth Rich's fund that the family started at Joel's request.

Rod sent a proposed contract to them in March, and the contract was signed by Joel, Mary and Aaron Rich. The contract said Rod can talk to the media since he is regularly on TV, but not on the family's behalf.

At the time, Rod said he was focused solely on finding a murder and only vaguely aware of the political implications of the case.

He spoke with Joel and Mary Rich, and they told him about relationships with Seth's girlfriend and his other friends. They also wanted him to speak with Aaron, Seth's brother, and Aaron's wife Molly, since Aaron and Seth were very close.

Aaron and Molly made it very clear to Rod that no matter turned up in the investigation, he should not talk to anyone about any emails that Seth may have sent from the DNC to Wikileaks.

"I asked why, why do you not want to talk to anyone about the emails, and they said because they were sure his death was not related to his job. I asked how they know that his death is not the result of emails, and Aaron said 'because we are telling you it is not,'" Rod Wheeler recounted.

During the first interview with Joe Capone, manager of the bar that Seth was dining at the night he died, Joe Capone told Rod that when he arrived for a "surprise" interview, Aaron had already called him ahead of time and told him that Rod was coming and not to talk to Rod about the emails.

When Rod went to interview Kelsey Mulka, Seth's girlfriend, he had the same greeting. She knew Rod would be calling because Aaron warned her. She said she was told by Aaron not to talk about the emails.

One interesting mention, she said Seth had issues with two supervisors at the DNC. She would not tell Rod their names, claiming Aaron told her not to talk about Seth's job.

In order to solve the case, whether it was job related or a botched street robbery or something else, Rod said he needed more information.

Aaron would not let Rod see Seth's personal computer, and said he already checked it.

Aaron would not let Rod see Seth's AT&T records or help him get the actual phone to look at who Seth had been

7605
Messages

Aaron would not let Rod see Seth's A&E records or help him get the actual phone to look at who Seth had been speaking to the night he died and in the weeks leading up to his death.

When Rod found out that Fox News was doing a story on Seth Rich related to a federal source who had seen emails between Seth Rich and Wikileaks, Rod called the chief of police in DC to inform him. He was connected to the director of Communications at the DC police department. Rod told him there was an FBI informant who had seen the emails. He got a telephone call 5 minutes after that from Det. DellaCamera, the lead detective on the murder investigation, and they planned to have a meeting Monday at the Library of Congress.

However, Detective DellaCamera never showed up for the meeting at the Library of Congress or returned Rod's calls after that.

DellaCamera had previously met Rod, but kept telling him that he cannot tell Rod anything about the case. Detective DellaCamera said he was told to "stand down" when it came to this case and not to talk about anything publicly. That is where they left it. Rod summarized DellaCamera's comments in a report.

Rod called Joel Rich on Monday at 5 pm to tell him that the story was coming out on Fox News, probably the new day. Joel said he already knew because a reporter from Fox had contacted him. Joel said he was encouraged by the new leads. He also suggested Rod contact an investigative reporter, Michelle Sigona, from CrimeWatch Daily with the information. But they agreed to wait until the Fox story comes out.

Rod also spoke with Aaron Rich, Joel's son, for 21 minutes the night before the story came out and told him about the new information that had emerged. Rod told Aaron the story that would likely be coming out in the near future.

Rod told both Aaron and Rich that he would be commenting on the case in the media and asking people to come forward if they had insight on the new information.

That afternoon, Rod contacted Marina Marraco, a reporter from Fox 5 DC. They had spoken previously about the story.

He told her about the Fox News story that was going to be published the next morning. She claimed to have heard about the story coming out, but said she wanted to talk to Rod in person about it.

She met him at a restaurant in DC. She asked him if can they could do an interview. He told her that he'd checked with a Fox News producer and the producer didn't want her to go with the story because it was a Fox News story. Marina promised it was just a "teaser" for the next day, and there would be good publicity as a result.

She got Rod to talk about the new information coming out the next day on Fox News. She had the camera rolling without telling Rod. She did not have the microphone up to his face, and so he didn't know she was recording.

Rod told her, thinking it was on background, that according to Fox News, an FBI agent provided credible information that the emails were sent from Seth Rich to Wikileaks. But he told her that he didn't have firsthand knowledge. However, Marina edited the video so it sounded like Rod had firsthand knowledge and had seen the emails himself.

Rod said, "I kept telling her, 'Marina, you cannot go with the story because this is the Fox News story. She said, 'no, I am not going to go with it. This is just going to be a teaser.'"

At 10 pm when the news comes on Fox 5, the story is the top story, positioned as an "exclusive breaking news" event, and not a teaser.

Marina is quoting Rod as if he was in a first person position of seeing Seth's computer. Rod maintains he never said what she reported.

Rod said: "Marina edited the audio so it looks like she is asking me if there is an FBI agent who confirmed emails were sent from Seth's computer to Wikileaks. She is only quoting me with part of what we talked about - 15 seconds of 3 minute conversation. She takes my statement out of context. She makes it sound like I am in a first person position, but that is because of where she started the tape. I told her during the video that I don't know where Seth's computers are stored; so if you hear that, then how is it I would have seen the email?"

Marina ran with the story, the story blew up. Rod texted her and confronted her about what she did, how she misrepresented herself and took his statements out of context. He asked her why she went with the story. He reminded her she didn't even get the email story from the firsthand source, but she made it sound like she did. She said that it doesn't matter, "If the camera was rolling, the camera was rolling."

Rod texted her that Fox News was upset by the story airing before theirs broke on the web site the next day.

She justified her actions saying, "The story has already blown up. This only gives credence to the story. If Fox News broke it, it would seem like conspiracy theory. Tomorrow will be huge for you guys, can't wait."

Rod said, "So Marina decided she would run with the story in her mind so it didn't seem like a conspiracy theory from Fox News. That backs up what I told her all along. That I told her not to go with this story."

Fox News, the national branch is upset, because the Fox 5 DC aired the story as the Fox 5 DC exclusive when it wasn't, Rod explained. Fox 5 "hadn't even investigated this thing," Rod said. But she ran with it as an exclusive story - as if it was hers.

((Det. DellaCamera calls Rod - call ends))



Messages

Received from maliamzimmerman@icloud.com on May 23, 2017 12:18:11 PM

#SETHRICHWAS A HERO

I KNOW THAT SETH RICH WAS INVOLVED IN THE DNC LEAK.

I know this because in late 2014 a person contacted me about helping me to start a branch of the Internet Party in the United States. He called himself Panda. I now know that Panda was Seth Rich.

Panda advised me that he was working on voter analytics tools and other technologies that the Internet Party may find helpful.

I communicated with Panda on a number of topics including corruption and the influence of corporate money in politics.

"He wanted to change that from the inside."

I was referring to what I knew when I did an interview with Bloomberg in New Zealand in May 2015. In that interview I hinted that Julian Assange and Wikileaks would release information about Hillary Clinton in the upcoming election.

The Rich family has reached out to me to ask that I be sensitive to their loss in my public comments. That request is entirely reasonable.

I have consulted with my lawyers. I accept that my full statement should be provided to the authorities and I am prepared to do that so that there can be a full investigation. My lawyers will speak with the authorities regarding the proper process.

If my evidence is required to be given in the United States I would be prepared to do so if appropriate arrangements are made. I would need a guarantee from Special Counsel Mueller, on behalf of the United States, of safe passage from New Zealand to the United States and back. In the coming days we will be communicating with the appropriate authorities to make the necessary arrangements. In the meantime, I will make no further comment.

STATEMENT FROM

KIM DOTCOM

Sent to Geoff Clark on May 24, 2017 5:56:25 AM

Thanks. Ron, Wikileaks is loosening up a little with trying to get info to us. Did you ask your attorney friend to try to get me something physical? Are you in New York? I want to share some things in person to give you more confidence.

Sent to Sean on May 26, 2017 1:53:43 PM

Heather, in our meeting I mentioned that Corey led in the report about the Russian collusion. Please ask Steve Zannon to call me so I can arrange to hand him everything that proves where the emails to Wikileaks are, how much was paid by Wikileaks to Seth Rich and his brother Aaron. We have an internal memo from a government agency showing Corey and Mr. Gebel (leaving name out on purpose).

Received from maliamzimmerman@icloud.com on Jun 6, 2017 9:55:02 AM

any other information, intelligence, documents or transactions that show Seth Rich and Wikileaks are connected would be helpful whether from law enforcement or the internet.

Received from maliamzimmerman@icloud.com on Jun 6, 2017 12:56:17 PM

Can you follow up with the Wikileaks people, and find out what they were supposed to get you? Nothing yet?

Sent to Rod Wheeler on Jun 13, 2017 3:22:22 PM

Just got done at fox 5.
In this story you said the above about learning about the emails between Wikileaks and Seth Rich.

Received from maliamzimmerman@icloud.com on Jun 14, 2017 7:25:48 PM

I would say that we should focus on getting whatever it was you are supposed to get from WikiLeaks and also Ron.

Received from maliamzimmerman@icloud.com on Jun 27, 2017 2:06:35 PM

also do you have time to check back with the guy tied to wikileaks and Ron about the FBI guy?

Received from Cassandra Fairbanks on Aug 1, 2017 2:59:00 PM

<http://bigleaguepolitics.com/audio-rod-wheeler-explains-fox-news-fiasco-claims-brother-blocked-wikileaks-inquiries/>

Received from Cassandra Fairbanks on Aug 1, 2017 3:59:29 PM

Who is speaking in the phone call about him being the WikiLeaks source?

Messages

Received from Cassandra Fairbanks on Aug 10, 2017 12:53:55 PM

So here's my story plan for today and tomorrow at one or both outlets:
 "How a Fake News Story Turned into a Real (Fake) Lawsuit" -- re: lawyer

"Walls Closing in on Russiagate Conspiracy Theorists: Evidence Mounts that DNC Emails Provided to Wikileaks by Inside Source" -- re: Newsweek and Nation articles

and

"Wheeler Admits on MSNBC That Lawsuit Has No Basis"

Received from Cassandra Fairbanks on Aug 18, 2017 8:55:39 PM

Nothing too exciting. Mostly just stuff about bannon. My interest is squarely on Seth/Russia/WikiLeaks

Sent to Cassandra Fairbanks on Aug 18, 2017 9:00:39 PM

Ed,

I'm not sure I even want to respond to you since you don't seem to have heard anything we have ever said to you! Since you have repeatedly accused me and my family, in both public and private venues, of having information related to Seth's murder that we're keeping secret, I feel compelled to try to respond.

Again your accusation is false and offensive! I am writing this to urge you to think carefully about how you would feel if someone did this to you, and to consider the harm you and your actions have and are causing my family, by pursuing this path that you seem to be hell bent on.

I know you are keen on wanting to prove Seth was a source of the emails to Wikileaks; and I believe, if you were an honest man, you would admit that you had that agenda when you first contacted us! You should be ashamed of your actions. To this date, despite your threatening texts and emails, no one, not even you, has presented us or the police with any evidence that supports your theory.

Instead all we get are threats from you (and others), conspiracy theories, and promises that someday soon, hidden evidence will be revealed.

As we've told you before, we will go where actual factual evidence takes us. If ever there is evidence regarding your conspiracy theory on our son Seth, we would accept it for what it is-but we're not going to accept lies.

Contrary to what you have been saying about our family, we want the truth and we will cherish our son and his memories for the wonderful young man he was.

You see Ed, that's the thing. We are interested in facts, not rumors or sensationalizing a story! Not rumors. Not third hand reports from anonymous sources within the FBI who are not revealed. Not promises of evidence soon to be revealed from cable hosts or Twitter want to be's. We want facts that are backed up by evidence.

That is what we wanted from the start, and we are tired of people trying to manipulate us to advance their own agendas. You should be ashamed to have come to us the way you did and claim to be an honest man!

A while back, you told me that your reporter friend at Fox had discovered evidence about the weapon and who had it. You said that it would disturb us, but that it was solid evidence, and you urged us to call her. So what did I do? I called her. And what was her disturbing evidence? She had none. She instead said that she had heard rumors that there was a break in to a car of an FBI agent in the vicinity of Seth's murder, and a gun that had gone missing could possibly have been related to the crime. But that break-in was previously reported and investigated. We never heard another word from you or anyone else about the gun that she said had gone missing. The truth is that every time you have claimed to have evidence, all we have gotten is rumors and theories. And when those theories do not pan out, you never admit you were wrong, or apologize for giving false info. To date, you have failed to deliver anything but pain and heartbreak.

I understand that you are now spreading rumors that Aaron was involved in one way or another. That claim is false, ridiculous actually, and I am certain you have no real evidence that backs up your rumour. Every time you repeat these false rumors, you are harming Aaron's reputation, risking his job prospects, and upsetting Mary and I by hurting the only son we have left.

As for the threats you say your family has received, we have said and done nothing to encourage threats to you or your family. To the contrary, we feel threats like those you were described to be disgusting. We condemn any person who would make them, and we hope that you have reported the threats to law enforcement so that they can find and punish whoever is involved.

As for us, Ed, enough is enough. I would ask you, out of respect for a family that has already lost a son and a brother, please leave us alone, stop saying false and hateful things about us and Aaron, and stop tampering our memory of Seth.

Joel Rich
 402-839-7763 Cell



Sent to **Cliff Floyd** on Aug 22, 2017 6:19:47 AM

On July 31, 2017, Rod Wheeler, through his counsel, provided David Folkenflik, reporter for National Public Radio ("NPR"), with the Complaint in this action to drive morning media coverage of the lawsuit the following day, when the Complaint would be filed. Wheeler, a veteran media contributor, and his counsel, Douglas Wigdor, a habitual media person, understood that the allegations they were about to make against Defendants Fox News, Maria Zimmerman, and Ed Butowsky, would inform the public's present demand for sensationalistic news and would dominate the news cycle on August 1, 2017. They were right.

On August 1, 2017, Wheeler filed the complaint with this Court dramatically alleging that the three Defendants colluded with President Trump and his Administration, to debunk the assertion that the Russian Government orchestrated the hacking of the Democratic National Committee ("DNC") by spinning a fake news story about the murder of former DNC staffer Seth Rich. The media coverage of the lawsuit was sweeping, and overwhelmingly negative toward the Defendants. Not surprisingly, the coverage centered almost exclusively on the conspiracy between the media conglomerate and the Administration to generate a fake news story in order to avoid a scandal, just as Wheeler and Wigdor hoped.

Afterward, however, Wheeler's claims have nothing to do with this spectacular conspiracy. Wheeler is suing Butowsky for defamation per se based on the purported misquoting of two quotes by Wheeler in a Fox News online publication by Defendant Maria Zimmerman. After peeling away the many layers of baseless, irrelevant rubbish, and understanding the context within which this case was brought, the frivolousness of this action becomes clear. In advance of filing this action, Wheeler, through his counsel, Douglas Wigdor, dangled the Complaint for weeks, threatening to sue Mr. Butowsky, and others, if the matter was not "resolved." The true target for Plaintiffs, however, was Fox News, playbacks off recent high-profile settlements by the Network involving sexual harassment and discrimination claims. Indeed, Wigdor's counsel has aggressively pursued a very public campaign against Fox News that has included press conferences with over a dozen former Fox News employees who were allegedly sexually harassed and discriminated against while they worked for the Network. He now has over twenty lawsuits filed or threatened against Fox News.

As noted in a recent New York Times article, Wigdor apparently employed a highly unusual, and questionable ethical strategy in recent weeks of attempting to settle all of these claims in one lump sum settlement, for which he would presumably be paid a fixed contingency fee. The claims range from sexual harassment to race discrimination, and include Wheeler's odd combination of a defamation and race discrimination claim. Wigdor contends that he can, without conflict, be the sole arbiter for apportioning this amount to his clients. Dismal.

Accounting for these other twenty-plus lawsuits puts Wigdor's motivation for making the Wheeler lawsuit his show pony into context.

Wigdor thought he could force a settlement using the pressure of the bad press. To that end, Wigdor has also inappropriately injected himself into the public approval process of a potential merger between Fox News and the UK's Sky TV, claiming that his lawsuits are a basis for UK regulators to reject the merger because they demonstrate a weakness in Fox News' internal controls.

The presence of allegations in the Complaint regarding this entirely unrelated issue would be surprising in any other case, not so here.

In truth, this lawsuit itself is plain, frivolous, and is being used as a pawn in a much broader game of chicken by Wheeler and his counsel. Wheeler participated in the story prior to being retained by the Rich family to investigate their son, and actively assisted Fox News in putting the story together for months prior to its publication. Wheeler then approved the story and the quotes attributed to him multiple times before the story was printed, after being asked by Mr. Zimmerman to "read it now" and to "please read it carefully." He even added language to one of the quotes, which was added by Mr. Zimmerman verbatim. Notably, the purported "lying" of Wheeler by Zimmerman and Butowsky in order to defame him is starkly contrasted by the meticulous effort by Zimmerman to obtain quotes from Wheeler, and get his approval for the story prior to publication.

Moreover, Wheeler made many, many statements before and after the publication showing exactly what was in his mind around the time that the article was published. For example, the day before publication, Wheeler spoke with a local Fox 5 DC reporter confirming that he had independent "sources at the FBI" that there is information that could link Seth Rich to Wikileaks. He also confirmed that he believed "there is a connection between the mayors office and the DNC, and that's the information that's going to come out tomorrow." The following day, after publication of the allegedly defamatory story, Wheeler confirmed with another media outlet that he had a "very credible" source confirming communications between Seth Rich and Wikileaks which led him "to think well perhaps there were some small communications between Seth and Wikileaks." He also claimed that "a high-ranking official at the DNC" was suspicious "hanging around" his investigation. These are just a few examples of his confirmatory statements made for weeks after the publication, and even during his media crusade after filing the Complaint.

Wheeler and his counsel have, of course, been well aware of these facts long before the filing of the Complaint.

They are also keenly aware that Ed Butowsky has retracted and repudiated the text messages and voicemail regarding the Administration's knowledge long before the filing of the Complaint. Butowsky's statements form the entire basis of the collusion claims by Wheeler. Without Butowsky's motivational untruths, the entire story falls apart.

As described in more detail below, this case represents the height of recklessness and abuse of the judicial system.

Wheeler and his counsel have used Defendant Ed Butowsky to siphon money from Fox News.

The case has no basis, and is clearly being advanced for an improper purpose – to harass, intimidate, and extort the Defendants in this case.

Wheeler and his counsel failed to make a reasonable inquiry into the facts of this case, and intentionally ignored counter-facts that exonerated the claims, such as Butowsky, nor Zimmerman have ever. It now seems no case communicated in anyway with the findings, in order to avoid a baseless conspiracy for broader gain. This conduct is sanctionable, and by this motion, Defendant Ed Butowsky seeks costs and attorney's fees.



btw, did you r friend ever offer anything from wikileaks?

<https://www.yahoo.com/news/wikileaks-faces-u-probes-2016-election-role-cia-173513427.html>

Any communications from congress about Wikileaks or Awan etc could have nothing to do with Seth rich.

THE UNIVERSITY OF CHICAGO PRESS

The paper is published by the International Union of Pure and Applied Chemistry.

The Inspector general in the house who discovered much of this through her audits, was viciously and maliciously attacked, sued, etc. She retired. She tried to pass this information to the deputy of Jeff Sessions at the DOJ, but was rebuffed.

[illegible]

US Rep. Schultz worked to shut down any investigation into Awan. She helped Imran Awan buy property in Pakistan and was compromised in other ways. She had a deeply personal relationship with him.

The NSA has messages in that regard, including some they didn't disclose in a recently released FOIA, showing communications between Seth Rich and Julian Assange. They are all designated SECRET or TOP SECRET. The NSA is an extremely over-censored, and also is not authorized to censor or subordinate anyone.

Speculation is the Pakistanis killed Seth Rich, because they were afraid that he was in a position to expose the Pakistani penetration of the networks. They were fearful of the exposure. Rather than take any risks, they got rid of him.

The final 1000-week high school course

Russia had actually "hacked" the DNC emails, than the National Security Agency would have had proof of such activity. In fact, the NSA could have tracked such activity. But they did not do that. That lack of evidence did not prevent a coordinated media campaign from spinning up to pin the blame on Russia for the "threat" and to portray Donald Trump as Putin's lackey and benefactor.

any effort to tell an alternative story has met with about opposition. Fox News, for example, came under withering fire after it published an article in May 2017 claiming that Seth Rich, a young Democrat operative, had leaked DNC emails to Julian Assange at WikiLeaks. The family of Seth Rich reached with fury and sued Fox, Matt Zimmerman and Ed Butowski, but that suit subsequently was dismissed.

Now there is new information, courtesy of the National Security Agency aka NSA, that confirms that the NSA has Top Secret and Secret documents that are responsive to a FOIA request for material on Scott Rich and his contacts with Julian Assange. While the content of these documents remain classified for now, they may provide documentary proof that Scott Rich "dropped the bomb" that alerts to Julian. If these documents are declassified, a big hole could be blown in the claim that Russia hacked the DNC.

P. Self-Rich was just a normal kid in the wrong place at the wrong time, his murder and untimely death would only have been a minor bop in the news cycle. Also a boy, it was a similar loss for the family and friends. But Self was not an ordinary kid. He worked for the Democratic National Committee aka the DNC and described himself as an "unclassified or uncorroborated data analyst" keen on making the world a better place.

Rich met a sudden and brutal end in a neighborhood near the U.S. Capitol in Washington, DC in the early hours of July 10, 2016. The initial report about the murder did not raise any political alarm in the United States. The CNN reporting of the murder was representative of the coverage at the time <<https://www.defense.greatpoint.com/v2?url?url=https://www.cnn.com/2016/07/11/politics/sarah-20rich-20killed-20washington/index.html&id=CNNLFPQ&src=cnnlfpq&src=www.20cnn.com/2016/07/11/politics/sarah-20rich-20killed-20washington/index.html&id=CNNLFPQ&src=cnnlfpq>>

Messages

zHfEn5g7fY8c7PbYD8EdY8m-qmCHGeadfMaZhdHXfDnHZe8YbG7aPm8Zn8x8t8c808e-LqWZ8t8f8K8u8l8-
 yZ8dH7w88m8t8b8Gf_A8f8b88E8U8e8-
 A Democratic National Committee employee died this weekend after he was shot in Northwest Washington.
 Seth Rich, 27, suffered multiple gunshot wounds early Sunday morning in Washington's Bloomingdale neighborhood,
 according to law enforcement officials.
 D.C. police said officers who had been patrolling the area responded to the sound of shots fired, ultimately finding
 Rich at the scene both "conscious and breathing." He was then transported to an area hospital, where police said he
 "succumbed to his injuries and was pronounced dead."
 Rich worked as voter expansion data director for the DNC since 2014, the DNC confirmed. A 2011 graduate of
 Creighton University, Rich's resume is filled with various jobs in Democratic politics and political consulting.
 But the circumstances and facts surrounding the murder were strange. Seth was shot in the back. Nothing was taken
 from his body—not his watch, not his wallet and not his credit cards. There was no obvious answer to the questions—
 who shot Seth and why?
 The interest in Seth's death took a dramatic turn when Wikileaks dumped the contents of DNC emails on its website
 on July 22, 2016. In order to put the Wikileaks theory regarding Seth's death in proper perspective, we must review
 events in the prior months connected to the Hillary Clinton and DNC email controversies.
 Seth Rich fell so deep in history, early or certainly, in need to the debate surrounding Hillary Clinton's missing and/or
 classified emails. During her time as Secretary of State, Hillary used a private server and sent thousands of messages
 over that server. This included emails containing Top Secret material.
 In May 2016, the State Department Inspector General added further fuel to the controversy by concluding that Hillary
 had violated State Department protocols and policies.
 The Inspector General was unable to find evidence that Clinton had ever sought approval from the State Department
 staff for her use of a private email server, determining that if Clinton had sought approval, Department staff would
 have declined her setup because of the "security risks in doing so." [54] As to the security risks, the report stated
 that "she did not comply with the Department's policies that were implemented in accordance with the Federal
 Records Act." [57]
 Public interest in Hillary's emails grew on June 12, 2016 when Wikileaks founder, Julian Assange, stated during an ITV
 interview: <https://uk.defense.proofpoint.com/v2/url?
 u=https://a...www.theguardian.com/media/2016/jun/12/wikileaks-2Dto-2Dpublish-2Dmore-2Dhillary-2Dclinton-2De-
 mails-2Dduran-2Dassange&d=DwMFaQ&c=cnx1hdOQpE0QpormZGwQ&e=qpUOMg7E8ogICDoyJ-
 zHfEn5g7fY8c7PbYD8EdY8m-qmCHGeadfMaZhdHXfDnHZe8YbG7aPm8Zn8x8t8c808e-LqWZ8t8f8K8u8l8-
 yZ8dH7w88m8t8b8Gf_A8f8b88E8U8e8-
 7HfEn5g7fY8c7PbYD8EdY8m-qmCHGeadfMaZhdHXfDnHZe8YbG7aPm8Zn8x8t8c808e-LqWZ8t8f8K8u8l8-
 yZ8dH7w88m8t8b8Gf_A8f8b88E8U8e8-
 "We have upcoming leaks in relation to Hillary Clinton... We have emails pending publication, that is correct," Assange
 said.
 Two days later (June 14) came news that the DNC computers had been "hacked" by the Russians. Ellen Nakamura, a
 Washington Post reporter <https://uk.defense.proofpoint.com/v2/url?
 u=https://a...www.washingtonpost.com/world/national-security/russian-2Dgovernment-2Dhackers-2Dpenetrated-
 2Ddnc-2Ddata-2Dopposition-2Dresearch-2Don-2Dtrump/2016/06/14/cf008c84-2D318e-2D71e8-2D31f7-2D7b6c19-
 88b79d-8fstory.html-2Dfutm-2Dterm-2D83bc888052485d-DwMFaQ&c=cnx1hdOQpE0QpormZGwQ&e=qpUOMg7E-
 8ogICDoyJ-
 zHfEn5g7fY8c7PbYD8EdY8m-qmCHGeadfMaZhdHXfDnHZe8YbG7aPm8Zn8x8t8c808e-LqWZ8t8f8K8u8l8-
 yZ8dH7w88m8t8b8Gf_A8f8b88E8U8e8-
 Crowdstrike, who had been hired by computer security company hired by the DNC—
 Crowdstrike—, wrote:
 Russian government hackers penetrated the computer network of the Democratic National Committee and gained
 access to the entire database of opposition research on GOP presidential candidate Donald Trump, according to
 committee officials and security experts who responded to the breach.
 The intruders so thoroughly compromised the DNC's system that they also were able to read all email and chat traffic,
 said DNC officials and the security experts.
 The intruder into the DNC was one of several targeting American political organizations. The networks of presidential
 candidate Hillary Clinton and Donald Trump were also targeted by Russian spies, as were the computers of some
 Republican political action committees, U.S. officials said, but details on those cases were not available.
 The Nakamura piece marked the first salvo in the Russian hacking drama. But the claim was not backed up by
 independently verified forensic evidence—it rested solely on the conclusions of a computer security company—
 Crowdstrike. The pro-Ukrainian politics of Crowdstrike's founder, Dmitri Alperovich, and his strident opposition to
 Russia cast a pall of bias over the findings of Crowdstrike. No U.S. Federal Law Enforcement official or agency was
 given access to the DNC servers. Neither the FBI nor Homeland Security were permitted to examine the servers and
 the alleged evidence of a hack. <https://uk.defense.proofpoint.com/v2/url?
 u=https://a...www.wired.com/2016/06/hack-2Ddnc-2Ddata-2Dresearch-2Ddnc-2Don-2Dtrump-2Dint_Kd-DwMFaQ&c-
 cnx1hdOQpE0QpormZGwQ&e=qpUOMg7E8ogICDoyJ-
 zHfEn5g7fY8c7PbYD8EdY8m-qmCHGeadfMaZhdHXfDnHZe8YbG7aPm8Zn8x8t8c808e-LqWZ8t8f8K8u8l8-
 yZ8dH7w88m8t8b8Gf_A8f8b88E8U8e8-
 Crowdstrike revealed that not one but two groups of hackers believed to be based in Russia had done just that. The
 intruders, according to Crowdstrike and the DNC officials who spoke to the Washington Post, fully accessed the
 campaign organization's emails and chats, and stole opposition research on Republi

Sent to Pablo Torre on Oct 30, 2018 5:39:03 AM

DNC Emails - A Seth Attack Not a Russian Hack

If Russia had actually "hacked" the DNC emails then the National Security Agency would have had proof of such
 activity. In fact, the NSA could have tracked such activity. But they did not do that. That lack of evidence did not
 prevent a coordinated media campaign from spinning up to pin the blame on Russia for the "theft" and to portray
 Donald Trump as Putin's lackey and beneficiary.

Any effort to tell an objective story has run with stout opposition. Fox News, for example, came under withering fire
 after it published an article in May 2017 claiming that Seth Rich, a young Democratic operative, had leaked DNC emails
 to Julian Assange at Wikileaks. The family of Seth Rich reacted with fury and sued Fox, Maria Zimmerman and Ed
 Butowsky, but that suit subsequently was dismissed.

Now there is new information, courtesy of the National Security Agency aka NSA, that confirms that the NSA has "Top
 Secret and Secret documents that are responsive to a FOIA request for material on Seth Rich and his contacts with
 Julian Assange. While the content of those documents remain classified for now, they may provide documentary proof
 that Seth Rich "dropped the bomb" on the emails to Julian. If those documents are declassified, a big hole could be blown in

CONFIDENTIAL

Mar 27, 2020 at 5:42:48 PM
 BUTOWSKY005573



1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000 1001 1002 1003 1004 1005 1006 1007 1008 1009 1010 1011 1012 1013 1014 1015 1016 1017 1018 1019 1020 1021 1022 1023 1024 1025 1026 1027 1028 1029 1030 1031 1032 1033 1034 1035 1036 1037 1038 1039 104

Russian government hackers penetrated the computer network of the Democratic National Committee and gained

Messages

committee officials and security experts who responded to the breach. The intruders so thoroughly compromised the DNC's system that they also were able to read all email and chat traffic, said DNC officials and the security experts. The intrusion into the DNC was one of several targeting American political organizations. The networks of presidential candidates Hillary Clinton and Donald Trump were also targeted by Russian spies, as were the computers of some Republican political action committees, U.S. officials said. But details on these cases were not available. The Bloomberg piece marked the first salvo in the Russian hacking drama. But the claim was not backed up by independently verified forensic evidence. It rested solely on the conclusions of a computer security company, Crowdfunder. The pro-Ukrainian policy of Crowdfunder's founder, Dmitri Alperovitch, and his strong opposition to Russia cast a pall over the findings of Crowdfunder. An U.S. Federal Law Enforcement official or agency was given access to the DNC servers. Neither the FBI nor Homeland Security were permitted to examine the servers and the alleged evidence of a hack. https://urldefense.proofpoint.com/v3/url?u=https-3A__www.foxtrad.com_2018-08-hack-20dnc-20brian-20russias-20breach-20dnc-20trump-20dirt_&d=DwNFwQ&e=cx%3D00QdFQqpsmZQwQ&r=agUQMgTE9agfCDayU-20HDEsWfT6Rc79DyD8EDh3em-0HGeadfMaZbxLNXEDvH2e8Y6G7eFmXQ2=0X1eG10&e-20E9GfQJmYH3BT%3D00Qs-1001A9gTgafAcade-

Crowdfunder revealed that not one but two groups of hackers believed to be based in Russia had done just that. The intruders, according to Crowdfunder and the DNC officials who spoke to the Washington Post, fully accessed the campaign organization's emails and chats, and stole opposition research on Republi

Sent to Scott Burns on Nov 29, 2018 2:12:14 PM

Google Brent Budowsky and WikiLeaks

Received from Trevor Fitzgibbons on Jan 2, 2019 5:41:06 PM

TF

i do pr - have represented numerous clients including Julian Assange and WikiLeaks as well as the Google foundation and films such as Dirty Wars by Jeremy Scahill - I also help companies launch products and authors launch books

Sent to Porter Berry on Feb 13, 2019 7:34:21 PM

WHY THE DNC WAS NOT HACKED BY THE RUSSIANS

By

William Binney

Larry Johnson

The FBI, CIA and NSA claim that the DNC emails published by WIKILEAKS on July 28, 2016 were obtained via a Russian hack, but more than three years after the alleged "hack" no forensic evidence has been produced to support that claim. In fact, the available forensic evidence contradicts the official account that blames the leak of the DNC emails on a Russian internet "intrusion". The existing evidence supports an alternative explanation--the files taken from the DNC on between 23 and 25 May 2016 and were copied onto a file storage device, such as a thumb drive.

If the Russians actually had conducted an internet based hack of the DNC computer network then the evidence of such an attack would have been collected and stored by the National Security Agency. The technical systems to accomplish this task have been in place since 2002. The NSA had an opportunity to make it clear that there was irrefutable proof of Russian meddling, particularly with regard to the DNC hack, when it signed on to the January 2017 "Intelligence Community Assessment," regarding Russian interference in the 2016 Presidential election.

We also assess Putin and the Russian Government aspired to help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him. All three agencies agree with this judgment. CIA and FBI have high confidence in this judgment; NSA has moderate confidence.

The phrase "moderate confidence" in intelligence speak for "we have no hard evidence." Thanks to the leaks by Edward Snowden, we know with certainty that the NSA had the capability to examine and analyze the DNC emails. NSA routinely "vacuumed up" email traffic transiting the U.S. using robust collection systems (whether or not anyone in the NSA chose to look for this data is another question). If those emails had been hacked over the internet then NSA also would have been able to track the electronic path they traveled over the internet. This kind of data would allow the NSA to declare without reservation or caveat that the Russians were guilty. The NSA could admit to such a fact in an unclassified assessment without compromising sources and methods. Instead, the NSA only claimed to have moderate confidence in the judgement regarding Russian meddling. If the NSA had hard intelligence to support the judgement the conclusion would have been stated as "full confidence."

We believe that Special Counsel Robert Mueller faces major embarrassment if he decides to pursue the indictment he filed--which accuses 12 Russian GRU military personnel and an entity identified as, Guccifer 2.0, for the DNC hack--because the available forensic evidence indicates the emails were copied onto a storage device.

According to a DOJ press release on the indictment of the Russians, Mueller declares that the emails were obtained via a "spearphishing" attack:

In 2016, officials in Unit 26166 began spearphishing volunteers and employees of the presidential campaign of Hillary Clinton, including the campaign's chairman. Through this process, officials in this unit were able to steal the usernames and passwords for numerous individuals and use those credentials to steal email content and hack into other computers. They also were able to hack into the computer networks of the Democratic Congressional Campaign Committee (DCCC) and the Democratic National Committee (DNC) through these spearphishing techniques to steal emails and documents, covertly monitor the computer activity of dozens of employees, and implant hundreds of files of malicious computer code to steal passwords and maintain access to these networks.

The officials in Unit 26166 coordinated with officials in Unit 34456 to plan the release of the stolen documents for the purpose of interfering with the 2016 presidential election. Defendants registered the domain DCLeaks.com and later staged the release of thousands of stolen emails and documents through that website. On the website, defendants claimed to be "American hacktivists" and used Facebook accounts with fictitious names and Twitter accounts to promote the website. After public accusations that the Russian government was behind the hacking of DNC and DCCC computers, defendants created the fictitious persona Guccifer 2.0. On the evening of June 16, 2016 between 8:19PM and 8:26PM, defendants used their Moscow-based server to search for a series of English words and phrases that later appeared in Guccifer 2.0's first blog post falsely claiming to be a lone Romanian hacker responsible for the hacks in the hopes of undermining the allegations of Russian involvement.

<https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offices-related-2016-election>

Notwithstanding the DOJ press release, an examination of the Wikileaks DNC files do not support the claim that the emails were obtained via spearphishing. Instead, the evidence clearly shows that the emails posted on the Wikileaks site were copied onto an electronic media, such as a CD-ROM or thumbdrive before they were posted at Wikileaks. The emails posted on Wikileaks were saved using the File Allocation Table (aka FAT) computer file system architecture.

An examination of the Wikileaks DNC files shows they were created on 23, 26 and 28 May respectively. The fact that they appear in a FAT system format indicates the data was transferred to a storage device, such as a thumb drive.

How do we know? The truth lies in the "last modified" time stamps on the Wikileaks files. Every single one of these time stamps end in even numbers. If you are not familiar with the FAT file system, you need to understand that when a date is stored under this system the data rounds the time to the nearest even numbered second.

We have examined 808 DNC email files stored at Wikileaks and all 808 files end in an even number - 2, 4, 6, 8 or 0. If a system other than FAT had been used, there would have been an equal probability of the time stamp ending with an odd number. But that is not the case with the data stored on the Wikileaks site. All end with an even number.

The DNC emails are in 3 batches (times are GMT).

Date	Count	Min Time	Max Time	FAT	Min Id	Max Id
2016-05-23	10520	02:12:38	02:45:47	x	3800	14319
2016-05-26	11958	06:21:30	06:04:36	x	1	22456
2016-05-28	12357	14:11:38	20:06:04	x	22457	44082

The random probability that FAT was not used is 1 chance in 2 to the 500th power or approximately 1 chance in 10 to the 150th power - in other words, an infinitely high order.

This data alone does not prove that the emails were copied at the DNC headquarters. But it does show that the data/emails posted by Wikileaks did go through a storage device, like a thumbdrive, before Wikileaks posted the emails on the World Wide Web.

This fact alone is enough to raise reasonable doubts about Mueller's indictment accusing 12 Russian soldiers as the authors of the leak of the DNC emails to Wikileaks. A soldier's defense attorney will argue, and rightly so, that someone

copied the DNC files to a storage device (e.g., USB thumb drive) and transferred that to WikiLeaks.

We also tested the hypothesis that WikiLeaks could have manipulated the files to produce the FAT result by comparing the DNC email files with the Podesta emails (aka Letter files) that were released on 21 September 2016. The FAT file format is NOT present in the Podesta files. If WikiLeaks employed a standard protocol for handling data(emails) received from unknown sources we should expect the file structure of the DNC emails to match the file structure of the Podesta emails. The evidence shows otherwise.

There is further compelling technical evidence that undermines the claim that the DNC emails were downloaded over the Internet as a result of a spearphishing attack. Bill Binney, a former Technical Director of the National Security Agency, along with other former intelligence community experts, examined emails posted by Guccifer 2.0 and discovered that those emails could not have been downloaded over the Internet as a result of a spearphishing attack. It is a simple matter of mathematics and physics.

Shortly after WikiLeaks announced it had the DNC emails, Guccifer 2.0 emerged on the public stage, claiming that "he" hacked the DNC and that he had the DNC emails. Guccifer 2.0 began in late June 2016 to publish documents as great that "he" had hacked from the DNC.

Taking Guccifer 2.0 at face value—i.e., that his documents were obtained via an Internet attack—Bill Binney conducted a forensic examination of the metadata contained in the posted documents based on Internet connection speeds in the United States. This analysis showed that the highest transfer rate was 49.1 megabytes per second, which is much faster than possible from a remote online connection. The 49.1 megabytes speed coincides with the download rate for a thumb drive.

Binney, assisted by other colleagues with technical expertise, extended the examination and ran various tests forensic from the Netherlands, Albania, Belgrade and the UK. The fastest rate obtained -- from a data center in New Jersey to a data center in the UK--was 12 megabytes per second, which is less than a fourth of the rate necessary to transfer the data, as it was listed from Guccifer 2.

The findings from the examination of the Guccifer 2.0 data and the WikiLeaks data does not prove who copied the information to a thumbdrive, but it does provide and empirical alternative explanation that undermines the Special Counsel's claim that the DNC was hacked. According to the forensic evidence for the Guccifer 2.0 data, the DNC emails were not taken by an Internet spearphishing attack. The data breach was local. It was copied from the network.

There is other circumstantial evidence that buttresses the conclusion that the data breach was a local effort that copied data.

First there is the Top Secret information leaked by Edward Snowden. If the DNC emails had been hacked via spearphishing (as alleged by Mueller) then the data would have been captured by the NSA by means of the Upstream program (Fairview, Stormbrew, Barney, Oakstar) and the forensic evidence would not modify times -- the data would be presented as sent.

Second, we have the public reporting on the DNC and Crowdstrike, which provide a bizarre timeline for the alleged Russian hacking.

It was 29 April 2016, when the DNC claims it became aware its servers had been penetrated (see <https://medium.com/homefront-rising/dumbtruck-how-crowdstrike-conned-america-on-the-back-of-the-dnc-e6fa52c0441>). No claim yet about who was responsible.

According to Crowdstrike founder, Dmitri Alperovitch, his company first detected the Russians mucking around inside the DNC server on 6 May 2016. A Crowdstrike intelligence analyst reportedly told Alperovitch that:

Falcon had identified not one but two Russian intruders: Cozy Bear, a group Crowdstrike's experts believed was affiliated with the FSB, Russia's answer to the CIA; and Fancy Bear, which they had linked to the GRU, Russian military intelligence.

<https://www.esquire.com/news-politics/a49902/the-russian-emigre-leading-the-fight-to-protect-america/>

Messages

And what did CrowdStrike do about this? Nothing. According to Michael Isikoff, CrowdStrike claimed their inactivity was a deliberate plan to avoid alerting the Russians that they had been "discovered." This is nonsense. If a security company detected a thief breaking into a house and stealing its contents, what sane company would counsel the client to do nothing in order to avoid alerting the thief? Utter nonsense.

We know from examining the Wikileaks data that the last message copied from the DNC network is dated Wed, 25 May 2016 06:48:35. No DNC emails were taken and released to Wikileaks after that date.

CrowdStrike waited until 10 June 2016 to take concrete steps to clean up the DNC network. Algerovitch told Esquire's Vicki Ward that:

Ultimately, the teams decided it was necessary to replace the software on every computer at the DNC. Until the network was clean, secrecy was vital. On the afternoon of Friday, June 10, all DNC employees were instructed to leave their laptops in the office.

<https://www.esquire.com/news-politics/a49002/the-russian-embryo-leading-the-fight-to-protect-america/>

Why does a cyber security company wait 45 days after allegedly uncovering a massive Russian attack on the DNC server to take concrete steps to safeguard the integrity of the information held on the server? This makes no sense.

A more plausible explanation is that it was discovered that emails had been downloaded from the server and copied onto a device like a thumbdrive. But the culprit had not yet been identified. We know one thing for certain: CrowdStrike did not take steps to shutdown and repair the DNC network until 18 days after the last email was copied from the server.

The final curiosity is that the DNC never provided the FBI access to its servers in order for qualified FBI technicians to conduct a thorough forensic examination. If this had been a genuine internet hack, it would be very easy for the NSA to identify when the information was taken and the route it moved after being hacked from the server. The NSA had the technical collection systems in place to enable analysts to know the date and time of the messages. But that has not been done.

Taken together, these disparate data points combine to paint a picture that exonerates alleged Russian hackers and implicates persons within our law enforcement and intelligence community taking part in a campaign of misinformation, deceit and disinformation. It is not a coincidence.



Sent to Catherine Herridge on Mar 27, 2019 7:17:02 AM

WHY THE DNC WAS NOT HACKED BY THE RUSSIANS

By
William Binney
Larry Johnson

The FBI, CIA and NSA claim that the DNC emails published by WIKILEAKS on July 28, 2016 were obtained via a Russian hack, but more than three years after the alleged "hack" no forensic evidence has been produced to support that claim. In fact, the available forensic evidence contradicts the official account that blames the leak on the DNC emails on a Russian internet "intrusion". The existing evidence supports an alternative explanation--the files taken from the DNC on between 23 and 25 May 2016 and were copied onto a file storage device, such as a thumb drive.

If the Russians actually had conducted an Internet based hack of the DNC computer network then the evidence of such an attack would have been collected and stored by the National Security Agency. The technical systems to accomplish this task have been in place since 2002. The NSA had an opportunity to make it clear that there was irrefutable proof of Russian meddling, particularly with regard to the DNC hack, when it signed on to the January 2017 "Intelligence Community Assessment," regarding Russian interference in the 2016 Presidential election.

We also assess Putin and the Russian Government aspired to help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him. All three agencies agree with this judgment. CIA and FBI have high confidence in this judgment; NSA has moderate confidence.

The phrase, "moderate confidence" is intelligence speak for "we have no hard evidence." Thanks to the leaks by Edward Snowden, we know with certainty that the NSA had the capability to examine and analyze the DNC emails. NSA routinely "vacuumed up" email traffic transiting the U.S. using robust collection systems (whether or not anyone in the NSA chose to look for this data is another question). If those emails had been hijacked over the internet, then NSA also would have been able to track the electronic path they traveled over the internet. This kind of data would allow the NSA to declare without reservation or caveat that the Russians were guilty. The NSA could admit to such a fact in an unclassified assessment without compromising sources and methods. Instead, the NSA only claimed to have moderate confidence in the judgment regarding Russian meddling. If the NSA had found intelligence to support

the judgement the conclusion would have been stated as "full confidence."

We believe that Special Counsel Robert Mueller faces major embarrassment if he decides to pursue the indictment he filed—which accuses 12 Russian GRU military personnel and an entity identified as, Guccifer 2.0, for the DNC hack—because the available forensic evidence indicates the emails were copied onto a storage device.

According to a DOJ press release on the indictment of the Russians, Mueller declares that the emails were obtained via a "spearphishing" attack:

In 2016, officials in Unit 26165 began spearphishing volunteers and employees of the presidential campaign of Hillary Clinton, including the campaign's chairman. Through that process, officials in this unit were able to steal the usernames and passwords for numerous individuals and use those credentials to steal email content and hack into other computers. They also were able to hack into the computer networks of the Democratic Congressional Campaign Committee (DCCC) and the Democratic National Committee (DNC) through these spearphishing techniques to steal emails and documents, covertly monitor the computer activity of dozens of employees, and implant hundreds of files of malicious computer code to steal passwords and maintain access to those networks.

The officials in Unit 26165 coordinated with officials in Unit 71465 to plan the release of the stolen documents for the purpose of interfering with the 2016 presidential election. Defendants registered the domain DCLocks.com and later staged the release of thousands of stolen emails and documents through that website. On the website, defendants claimed to be "American hackers" and used Facebook accounts with fictitious names and Twitter accounts to promote the website. After public accusations that the Russian government was behind the hacking of DNC and DCCC computers, defendants created the fictitious persona Guccifer 2.0. On the evening of June 15, 2016 between 4:13PM and 4:30PM, defendants used their Moscow-based server to search for a series of English words and phrases that later appeared in Guccifer 2.0's first blog post, falsely claiming to be a lone Russian hacker responsible for the hacks in the hopes of undermining the allegations of Russian involvement.

<https://www.justice.gov/patrigrand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election>

Notwithstanding the DOJ press release, an examination of the Wikileaks DNC files do not support the claim that the emails were obtained via spearphishing. Instead, the evidence clearly shows that the emails posted on the Wikileaks site were copied onto an electronic media, such as a CD-ROM or thumbdrive before they were posted at Wikileaks. The emails posted on Wikileaks were saved using the File Allocation Table (aka FAT) computer file system architecture.

An examination of the Wikileaks DNC files shows they were created on 23, 25 and 26 May respectively. The fact that they appear in a FAT system format indicates the data was transferred to a storage device, such as a thumb drive.

How do we know? The truth lies in the "last modified" time stamps on the Wikileaks files. Every single one of these time stamps ends in even numbers. If you are not familiar with the FAT file system, you need to understand that when a date is stored under this system the date rounds the time to the nearest even numbered second.

We have examined 600 DNC email files stored on Wikileaks and all 600 files end in an even number—2, 4, 6, 8 or 0. If a system other than FAT had been used, there would have been an equal probability of the time stamp ending with an odd number. But that is not the case with the data stored on the Wikileaks site. All end with an even number.

The DNC emails are in 3 batches (times are GMT).

Date	Count	Min Time	Max Time	FAT	Min id	Max id
2016-05-23	10520	02:12:58	02:45:42 x	3630	14378	
2016-05-25	11958	06:21:30	06:34:36 x	1	22488	
2016-05-26	13357	14:11:36	20:06:04 x	22457	64053	

The random probability that FAT was not used is 1 chance in 2 to the 500th power or approximately 1 chance in 10 to the 150th power – in other words, an infinitely high order.

This data alone does not prove that the emails were copied at the DNC headquarters. But it does show that the data emails posted by Wikileaks did go through a storage device, like a thumbdrive, before Wikileaks posted the emails on the World Wide Web.

This fact alone is enough to raise reasonable doubts about Mueller's indictment accusing 12 Russian soldiers as the suspects for the leak of the DNC emails to Wikileaks. A savvy defense attorney will argue, and rightly so, that someone copied the DNC files to a storage device (E.g., USB thumb drive) and transferred that to Wikileaks.

We also tested the hypothesis that Wikileaks could have manipulated the files to produce the FAT result by comparing the DNC email files with the Podesta emails (aka Carter files) that was released on 21 September 2016. The FAT file format is NOT present in the Podesta files. If Wikileaks employed a standard protocol for handling data emails received from unknown sources we should expect the file structure of the DNC emails to match the file structure of the Podesta emails. The evidence shows otherwise.

There is further compelling technical evidence that undermines the claim that the DNC emails were downloaded over the internet as a result of a spearphishing attack. Bill Binney, a former Technical Director of the National Security Agency, along with other former intelligence community experts, examined emails posted by Guccifer 2.0 and discovered that those emails could not have been downloaded over the internet as a result of a spearphishing attack. It is a simple matter of mathematics and physics.

Shortly after Wikileaks announced it had the DNC emails, Guccifer 2.0 emerged on the public stage, claiming that "he" hacked the DNC and that he had the DNC emails. Guccifer 2.0 began in late June 2016 to publish documents as proof that "he" had hacked from the DNC.

Taking Guccifer 2.0 at face value—i.e., that his documents were obtained via an internet attack—Bill Binney conducted a forensic examination of the metadata contained in the posted documents based on internet connection

Messages

speeds in the United States. The analysis showed that the highest transfer rate was 49.1 megabytes per second, which is much faster than possible from a remote online connection. The 49.1 megabytes speed coincides with the download rate for a thumb drive.

Binney, assisted by other colleagues with technical expertise, extended the examination and ran various tests forensic from the Netherlands, Albania, Belgrade and the UK. The fastest rate obtained -- from a data center in New Jersey to a data center in the UK--was 12 megabytes per second, which is less than a fourth of the rate necessary to transfer the data, as it was taken from October 2.

The findings from the examination of the Guccifer 2.0 data and the Wikileaks data does not prove who copied the information to a thumbdrive, but it does provide an empirical alternative explanation that undermines the Special Counsel's claim that the DNC was hacked. According to the forensic evidence for the Guccifer 2.0 data, the DNC emails were not taken by an Internet spearphishing attack. The data breach was local. It was copied from the network.

There is other circumstantial evidence that buttresses the conclusion that the data breach was a local effort that copied data.

First there is the Top Secret information leaked by Edward Snowden. If the DNC emails had been hacked via spearphishing (as alleged by Mueller) then the data would have been captured by the NSA by means of the Upstream program (Fairview, Stormbrew, Barney, Oakstar) and the forensic evidence would not modify times -- the data would be presented as sent.

Second, we have the public reporting on the DNC and Crowdstrike, which provide a bizarre timeline for the alleged Russian hacking.

It was 29 April 2016, when the DNC claims it became aware its servers had been penetrated (see <https://medium.com/humaintel-rising/dumbstruck-how-crowdstrike-conned-america-on-the-hack-of-the-dnc-ecfa52216411>). No claim yet about who was responsible.

According to Crowdstrike founder, Dmitri Alperovitch, his company first detected the Russians mucking around inside the DNC server on 6 May 2016. A Crowdstrike intelligence analyst reportedly told Alperovitch that:

Falcon had identified not one but two Russian intruders: Cozy Bear, a group Crowdstrike's experts believed was affiliated with the FSB, Russia's answer to the CIA; and Fancy Bear, which they had linked to the GRU, Russian military intelligence.

(<https://www.esquire.com/news-politics/a48902/the-russian-emigre-leading-the-fight-to-protect-america/>)

And what did Crowdstrike do about this? Nothing. According to Michael Isikoff, Crowdstrike claimed their inactivity was a deliberate plan to avoid alerting the Russians that they had been "discovered." This is nonsense. If a security company detected a thief breaking into a house and stealing its contents, what sane company would counsel the client to do nothing in order to avoid alerting the thief? Lame response.

We know from examining the Wikileaks data that the last message copied from the DNC network is dated Wed, 26 May 2016 03:49:35. No DNC emails were taken and released to Wikileaks after that date.

Crowdstrike waited until 10 June 2016 to take concrete steps to clean up the DNC network. Alperovitch told Esquire's Vicky Ward that:

Ultimately, the teams decided it was necessary to replace the software on every computer at the DNC. Until the network was clean, security was vital. On the afternoon of Friday, June 10, all DNC employees were instructed to leave their laptops in the office.

(<https://www.esquire.com/news-politics/a48902/the-russian-emigre-leading-the-fight-to-protect-america/>)

Why does a cyber security company wait 45 days after allegedly uncovering a massive Russian attack on the DNC server to take concrete steps to safeguard the integrity of the information held on the server? This makes no sense.

A more plausible explanation is that it was discovered that emails had been downloaded from the server and copied onto a device like a thumbdrive. But the culprit had not yet been identified. We know one thing for certain--

Crowdstrike did not take steps to shutdown and repair the DNC network until 19 days after the last email was copied from the server.

The final curiosity is that the DNC never provided the FBI access to its servers in order for qualified FBI technicians to conduct a thorough forensic examination. If this had been a genuine Internet hack, it would be very easy for the NSA to identify when the information was taken and the route it moved after being hacked from the server. The NSA had the technical collection systems in place to enable analysts to know the date and time of the messages. But that has not been done.

Taken together, these disparate data points combine to paint a picture that exonerates alleged Russian hackers and implicates persons within our law enforcement and intelligence community taking part in a campaign of misinformation, deceit and incompetence. It is not a pretty picture.

On Feb 13, 2018, at 8:12 PM, Ty Clevenger <tyclevenger@yahoo.com> wrote:

I think it's good. I highlighted a couple of words ("data" and "data") that may have been interchanged, but everything else looks great.

On Tuesday, February 12, 2019, 2:03:19 PM EST, Larry Johnson <ljohnson1@enc.com> wrote:

Wanted to keep you guys updated on the place that is in draft. Please read and let me know your thoughts.

The FBI, CIA and NSA claim that the DNC emails published by WikiLeaks on June 2016 were obtained from

Russian hack, but they have provided no forensic evidence to support that claim. An examination of the forensic evidence directly undermines the claim of the intelligence/law enforcement community and supports the hypothesis that the files taken from the DNC on the 25th of May 2016 were copied onto a file storage device, such as a thumb drive. If the Russians actually had conducted an internet based hack of the DNC computer network then the evidence of such an attack would have been collected and stored by the National Security Agency. The technical systems to accomplish this task have been in place since 2002. It is worth noting the rapid endorsement that the NSA gave with the judgement in the January 2017 "Intelligence Community Assessment," regarding Russian interference in the 2016 Presidential election.

We also assess Putin and the Russian Government aspired to help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him. All three agencies agree with this judgment. CIA and FBI have high confidence in this judgment; NSA has moderate confidence.

In light of the established capability of the NSA to collect compromising evidence for this particular judgment, the phrase, "moderate confidence" is a clear indicator that the NSA had not examined any of the emails from the alleged DNC "hack" and asked them to Russian agents. Had they done so, there would be no doubt about Russian culpability. And the NSA could make such a declaratory judgment in an unclassified assessment without compromising sources and methods. This is the equivalent of the dog that did not bark.

We believe that Special Counsel Robert Mueller faces major embarrassment if he decides to pursue the indictment he filed, which names 12 Russian GRU military personnel and a person identified as, Guccifer 2.0, as the ones responsible for the DNC hack. According to a DOJ press release on the indictment, Mueller claims the emails were obtained via a "spearphishing" attack.

In 2016, officials in Unit 28166 began spearphishing volunteers and employees of the presidential campaign of Hillary Clinton, including the campaign's chairman. Through that process, officials in this unit were able to steal the usernames and passwords for numerous individuals and use those credentials to steal email content and hack into other computers. They also were able to hack into the computer networks of the Democratic Congressional Campaign Committee (DCCC) and the Democratic National Committee (DNC) through these spearphishing techniques to steal emails and documents, covertly monitor the computer activity of dozens of employees, and implant hundreds of files of malicious computer code to steal passwords and maintain access to those networks.

The officials in Unit 28166 coordinated with officials in Unit 74456 to plan the release of the stolen documents for the purpose of interfering with the 2016 presidential election. Defendants registered the domain DCLinks.com and later staged the release of thousands of stolen emails and documents through that website. On the website, defendants claimed to be "American hackers" and used Facebook accounts with fictitious names and Twitter accounts to promote the website. After public accusations that the Russian government was behind the hacking of DNC and DCCC computers, defendants created the fictitious persona Guccifer 2.0. On the evening of June 15, 2016 between 4:10PM and 4:00PM, defendants used their Moscow-based server to search for a series of English words and phrases that later appeared in Guccifer 2.0's first blog post falsely claiming to be a lone Romanian hacker responsible for the hacks in the hopes of undermining the allegations of Russian involvement.

(<https://www.justice.gov/opa/briand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election>)

Notwithstanding the DOJ press release, an examination of the Wikileaks DNC files do not support the claim that the emails were obtained via spearphishing. Instead, the evidence clearly shows that the emails posted on the Wikileaks site were copied onto an electronic media, such as a CD-ROM or thumbdrive before they were posted at Wikileaks.

We have examined the Wikileaks DNC files, which were actually created on 23, 25 and 26 May. In other words, those emails were copied on three different dates. Use of the FAT system indicates data transfer to a storage device, such as a thumb drive.

How do we know? The truth lies in the "last modified" time stamps on the Wikileaks files. Every single one of these time stamps end in even numbers. If you are not familiar with the FAT file system, you must understand that when data is stored under this system the data rounds the time to the nearest even numbered second.

We have examined 500 DNC email files stored on Wikileaks and all 500 files end in an even number - 2, 4, 6, 8 or 0. If a system other than FAT had been used, there would have been an equal probability of the time stamp ending with an odd number. But that is not the case with the data stored on the Wikileaks site. All end with an even number.

The DNC emails are in 4 batches (times are GMT):

Date	Count	Min Time	Max Time	FAT	Min	Max	id
2016-05-23	10420	03:12:38	03:45:42 x	3800	14310		
2016-05-25	11396	05:21:30	06:04:38 x	1	22458		
2016-05-26	13357	14:11:36	20:06:04 x	22457	44053		

Messages

The random probability that FAT was not used is 1 chance in 2 to the 500th power or approximately 1 chance in 10 to the 150th power – in other words, an infinitesimal of higher order.

This does not prove that the emails were copied at the DNC headquarters. But it does prove that the data/emails posted by WikiLeaks did go through a storage device, like a thumbdrive, before WikiLeaks posted the emails on the World Wide Web.

If Mueller tries to bring this case against the 12 Russian soldiers to Court,

he will need to provide evidence that the storage device was not connected to the DNC local network. Otherwise, the defense will argue, and rightly so, that someone copied the DNC files to a storage device (Eg., USB thumb drive) and transferred that to WikiLeaks.

We also tested the hypothesis that WikiLeaks could have manipulated the files to produce the FAT result by comparing the DNC email files with the Podesta emails (aka Letter file) that was released on 21 September 2016. The FAT file format is NOT present in the Podesta files. If WikiLeaks employed a standard protocol for handling data/emails received from unknown sources then it would be sensible to conclude that the file structure of the DNC emails matched the file structure of the Podesta emails.

But the evidence shows otherwise.

Bill Binney, a former Technical Director of the National Security Agency, along with other former intelligence community experts, examined emails posted by Guccifer 2.0 and discovered that those emails could not have been downloaded over the internet as a result of a spearphishing attack. It is a simple matter of mathematics and physics.

Shortly after WikiLeaks announced it had the DNC emails, Guccifer 2.0 emerged on the public stage, claiming that he hacked the DNC and that he had the DNC emails. Guccifer 2.0 began in late June 2016 to publish documents as proof that "he" had hacked from the DNC.

Taking Guccifer 2.0 at face value—i.e., that his documents were obtained via an internet attack—Bill Binney conducted a forensic examination of the metadata contained in the posted documents based on internet connection speeds in the United States. This analysis showed that the highest transfer rate was 49.1 megabytes per second, which is much faster than possible from a remote online connection.

Bill Binney and other colleagues with technical expertise extended the examination and ran various tests forensic from the Netherlands, Albania, Belgrade and the UK. The fastest rate obtained -- from a data center in New Jersey to a data center in the UK--was 12 megabytes per second, which is less than a fourth of the rate necessary to transfer the data, as it was listed from Guccifer 2.

The 49.1 megabytes speed coincides with the download rate for a thumb drive.

The findings from the examination of the Guccifer 2.0 data and the WikiLeaks data does not prove who was responsible for copying the information to a thumbdrive but it does refute the Special Counsel's claim that the DNC was hacked. It was not an internet spearphishing attack. The data breach was local. It was copied from the network.

There is other circumstantial evidence that buttresses the conclusion that the data breach was a local effort that copied data.

First there is the Top Secret information leaked by Edward Snowden. If the DNC emails had been hacked via spearphishing (as alleged by Mueller), then the data would have been captured by the NSA by means of the Upstream program [Fairview, Stormbrew, Blarney, Oakstar] and the forensic evidence would not modify times - the data would be presented as sent.

Second, we have the public reporting on the DNC and Cambridge, which provide a bizarre timeline for the alleged Russian hacking.

It was 29 April 2016, when the DNC claims it became aware its servers had been penetrated (see <https://medium.com/homefront-rising/dumbstruck-how-crowdstrike-conned-america-on-the-back-of-the-dnc-ecfa522ff411>). No claim yet about who was responsible.

According to CrowdStrike founder, Dmitri Alperovich, his company first detected the Russians mucking around inside the DNC server on 6 May 2016. A CrowdStrike intelligence analyst reportedly told Alperovich that:

Falcon had identified not one but two Russian intruders: Coby Bear, a group CrowdStrike's experts believed was affiliated with the FSB, Russia's answer to the CIA; and Fancy Bear, which they had linked to the GRU, Russian military intelligence.

Messages

<https://www.esquire.com/news-politics/a48802/the-russian-emigre-leading-the-fight-to-protect-america/>

And what did CrowdStrike do about this? Nothing. According to Michael Isikoff, CrowdStrike claimed their inactivity was a deliberate plan to avoid alerting the Russians that they had been "discovered." This is nonsense. If you discovered a thief breaking into your house and who was in the process of stealing its contents, what sane law enforcement officer would counsel doing nothing in order to avoid alerting the thief? Utter nonsense.

We know from examining the Wikileaks data that the last message copied from the DNC network is dated Wed, 26 May 2016 08:48:35. No emails were taken and released to Wikileaks after that date.

CrowdStrike waited until 10 June 2016 to take concrete steps to clean up the DNC network. Alperovitch told Esquire's Vicky Ward that:

Ultimately, the team decided it was necessary to replace the software on every computer at the DNC. Until the network was clean, secrecy was vital. On the afternoon of Friday, June 10, all DNC employees were instructed to leave their laptops in the office.

<https://www.esquire.com/news-politics/a48802/the-russian-emigre-leading-the-fight-to-protect-america/>

Why does a cyber security company wait 45 days after allegedly uncovering a massive Russian attack on the DNC server to take concrete steps to safeguard the integrity of the information held on the server? This makes no sense.

A more plausible explanation is that it was discovered that emails had been downloaded from the server and copied onto a device like a thumbdrive. But the culprit had not yet been identified. We know one thing for certain—CrowdStrike did not take steps to shutdown and repair the DNC network until 16 days after the last email was copied from the server.

The final curiosity is that the DNC never provided the FBI access to its servers in order for qualified FBI technicians to conduct a thorough forensic examination. If this had been a genuine internet hack, it would be very easy for the NSA to identify when the information was taken and the route it moved after being hacked from the server. The NSA had the technical collection systems in place to enable analysts to know the date and time of the messages. But that has not been done.

Taken together, these disparate data points combine to paint a picture that exonerates alleged Russian hackers and implicates our law enforcement and intelligence community in a campaign of misinformation, deceit and



Sent to Ed Henry on Mar 27, 2019 1:29:14 PM

WHY THE DNC WAS NOT HACKED BY THE RUSSIANS

By
William Binney
Larry Johnson

The FBI, CIA and NSA claim that the DNC emails published by WIKILEAKS on July 28, 2016 were obtained via a Russian hack, but more than three years after the alleged "hack" no forensic evidence has been produced to support that claim. In fact, the available forensic evidence contradicts the official account that blames the leak of the DNC emails on a Russian internet "intrusion". The existing evidence supports an alternative explanation—the files taken from the DNC on between 23 and 25 May 2016 and were copied onto a file storage device, such as a thumb drive.

If the Russians actually had conducted an internet based hack of the DNC computer network then the evidence of such an attack would have been collected and stored by the National Security Agency. The technical systems to accomplish this task have been in place since 2002. The NSA had an opportunity to make it clear that there was irrefutable proof of Russian meddling, particularly with regard to the DNC hack, when it signed on to the January 2017 "Intelligence Community Assessment," regarding Russian interference in the 2016 Presidential election.

We also accuse Putin and the Russian Government applied to help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him. All three agencies agree with this judgment. CIA and FBI have high confidence in this judgment; NSA has moderate confidence.

The phrase, "moderate confidence" is intelligence speak for "we have no hard evidence." Thanks to the leaks by Edward Snowden, we know with certainty that the NSA had the capability to examine and analyze the DNC emails. NSA routinely "vacuumed up" email traffic transiting the U.S. using robust collection systems (whether or not anyone in the NSA chose to look for this data is another question). If these emails had been hijacked over the internet then NSA also would have been able to track the electronic path they traveled over the internet. This kind of data would allow the NSA to declare without reservation or caveat that the Russians were guilty. The NSA could admit to such a fact in an unclassified assessment without compromising sources and methods. Instead, the NSA only claimed to have moderate confidence in the judgement regarding Russian meddling. If the NSA had had intelligence to support the judgement the conclusion would have been stated as "full confidence."

We believe that Special Counsel Robert Mueller faces major embarrassment if he decides to pursue the indictment he filed—which accuses 12 Russian GRU military personnel and an entity identified as, Guccifer 2.0, for the DNC hack—because the available forensic evidence indicates the emails were copied onto a storage device.

Messages

According to a DOJ press release on the indictment of the Russians, Mueller declares that the emails were obtained via a "spearphishing" attack:

In 2016, officials in Unit 26165 began spearphishing volunteers and employees of the presidential campaign of Hillary Clinton, including the campaign's chairman. Through that process, officials in this unit were able to steal the usernames and passwords for numerous individuals and use those credentials to steal email content and hack into other computers. They also were able to hack into the computer networks of the Democratic Congressional Campaign Committee (DCCC) and the Democratic National Committee (DNC) through these spearphishing techniques to steal emails and documents, covertly monitor the computer activity of dozens of employees, and implant hundreds of files of malicious computer code to steal passwords and maintain access to those networks.

The officials in Unit 26165 coordinated with officials in Unit 71455 to plan the release of the stolen documents for the purpose of interfering with the 2016 presidential election. Defendants registered the domain DCLeaks.com and later staged the release of thousands of stolen emails and documents through that website. On the website, defendants claimed to be "American hacktivists" and used Facebook accounts with fictitious names and Twitter accounts to promote the website. After public accusations that the Russian government was behind the hacking of DNC and DCCC computers, defendants created the fictitious persona Guccifer 2.0. On the evening of June 15, 2016 between 4:19PM and 4:56PM, defendants used their Moscow-based server to search for a series of English words and phrases that later appeared in Guccifer 2.0's first blog post falsely claiming to be a lone Romanian hacker responsible for the hacks in the hopes of undermining the allegations of Russian involvement. (<https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election>)

Notwithstanding the DOJ press release, an examination of the Wikileaks DNC files do not support the claim that the emails were obtained via spearphishing. Instead, the evidence clearly shows that the emails posted on the Wikileaks site were copied onto an electronic media, such as a CD-ROM or thumbdrive before they were posted at Wikileaks. The emails posted on Wikileaks were saved using the File Allocation Table (aka FAT) computer file system architecture.

An examination of the Wikileaks DNC files shows they were created on 23, 25 and 26 May respectively. The fact that they appear in a FAT system format indicates the data was transferred to a storage device, such as a thumb drive.

How do we know? The truth lies in the "last modified" time stamps on the Wikileaks files. Every single one of these time stamps ends in even numbers. If you are not familiar with the FAT file system, you need to understand that when a date is stored under this system the time to the nearest even numbered second.

We have examined 800 DNC email files stored on Wikileaks and all 800 files end in an even number—2, 4, 6, 8 or 0. If a system other than FAT had been used, there would have been an equal probability of the time stamp ending with an odd number. But that is not the case with the data stored on the Wikileaks site. All end with an even number.

The DNC emails are in 3 batches (times are GMT):

Date	Count	Min Time	Max Time	FAT Min	Max
2016-05-23	10520	02:12:38	02:45:42 x	3800	14318
2016-05-25	11936	06:21:30	06:04:36 x	1	22458
2016-05-26	19357	14:11:36	20:06:04 x	22457	44062

The random probability that FAT was not used is 1 chance in 2 to the 500th power or approximately 1 chance in 10 to the 150th power – in other words, an infinitely high order.

This data alone does not prove that the emails were copied at the DNC headquarters. But it does show that the data/emails posted by Wikileaks did go through a storage device, like a thumbdrive, before Wikileaks posted the emails on the World Wide Web.

This fact alone is enough to raise reasonable doubts about Mueller's indictment accusing 12 Russian soldiers as the culprits for the leak of the DNC emails to Wikileaks. A savvy defense attorney will argue, and rightly so, that someone copied the DNC files to a storage device (e.g., USB thumb drive) and transferred that to Wikileaks.

We also tested the hypothesis that Wikileaks could have manipulated the files to produce the FAT result by comparing the DNC email files with the Podesta emails (aka Carter files) that was released on 21 September 2016. The FAT file format is NOT present in the Podesta files. If Wikileaks employed a standard protocol for handling data/emails received from unknown sources we should expect the file structure of the DNC emails to match the file structure of the Podesta emails. The evidence shows otherwise.

There is further compelling technical evidence that undermines the claim that the DNC emails were downloaded over the internet as a result of a spearphishing attack. Bill Binnay, a former Technical Director of the National Security Agency, along with other former intelligence community experts, examined emails posted by Guccifer 2.0 and discovered that those emails could not have been downloaded over the internet as a result of a spearphishing attack. It is a simple matter of mathematics and physics.

Shortly after Wikileaks announced it had the DNC emails, Guccifer 2.0 emerged on the public stage, claiming that "he" hacked the DNC and that he had the DNC emails. Guccifer 2.0 began in late June 2016 to publish documents as proof that "he" had hacked from the DNC.

Taking Guccifer 2.0 at face value (i.e., that his documents were obtained via an internet attack), Bill Binnay conducted a forensic examination of the metadata contained in the posted documents based on internet connection speeds in the United States. This analysis showed that the highest transfer rate was 49.1 megabytes per second, which is much faster than possible from a remote online connection. The 49.1 megabytes speed coincides with the download rate for a thumb drive.

Binnay, assisted by other colleagues with technical expertise, extended the examination and ran various tests for cables from the Netherlands, Albania, Bulgaria and the UK. The fastest rate obtained – from a data center in New Jersey to

a data center in the UK--was 12 megabytes per second, which is less than a tenth of the rate necessary to transfer the data, as it was filed from Guccifer 2.

The findings from the examination of the Guccifer 2.0 data and the Wikileaks data does not prove who copied the information to a thumbdrive, but it does provide an empirical alternative explanation that undermines the Special Counsel's claim that the DNC was hacked. According to the forensic evidence for the Guccifer 2.0 data, the DNC emails were not taken by an internet spearphishing attack. The data breach was local. It was copied from the network.

There is other circumstantial evidence that buttresses the conclusion that the data breach was a local effort that copied data.

First there is the Top Secret information leaked by Edward Snowden. If the DNC emails had been hacked via spearphishing (as alleged by Mueller) then the data would have been captured by the NSA by means of the Upstream program (Fairview, Stormbrew, Blarney, Oakstar) and the forensic evidence would not modify times - the data would be presented as sent.

Second, we have the public reporting on the DNC and Crowdstrike, which provide a discrete timeline for the alleged Russian hacking.

It was 29 April 2016, when the DNC claims it became aware its servers had been penetrated (see <https://medium.com/homefront-rising/dumbstruck-how-crowdstrike-conned-america-on-the-hack-of-the-dnc-ecfa527f4411>). No claim yet about who was responsible.

According to Crowdstrike founder, Dimitri Alperovitch, his company first detected the Russians mucking around inside the DNC server on 6 May 2016. A Crowdstrike intelligence analyst reportedly told Alperovitch that:

Falcon had identified not one but two Russian intruders: Cozy Bear, a group Crowdstrike's experts believed was affiliated with the FSB, Russia's answer to the CIA; and Fancy Bear, which they had linked to the GRU, Russian military intelligence. (<https://www.esquire.com/news-politics/a49902/the-russian-amigre-leading-the-fight-to-protect-america/>)

And what did Crowdstrike do about this? Nothing. According to Michael Isikoff, Crowdstrike claimed their inactivity was a deliberate plan to avoid alerting the Russians that they had been "discovered." This is nonsense. If a security company detected a thief breaking into a house and stealing its contents, what sane company would counsel the effort to do nothing in order to avoid alerting the thief? Utter nonsense.

We know from examining the Wikileaks data that the last message copied from the DNC network is dated Wed, 25 May 2016 06:43:35. No DNC emails were taken and released to Wikileaks after that date.

Crowdstrike waited until 10 June 2016 to take concrete steps to clean up the DNC network. Alperovitch told Esquire's Vicky Ward that:

Ultimately, the team decided it was necessary to replace the software on every computer at the DNC. Until the network was clean, secrecy was vital. On the afternoon of Friday, June 10, all DNC employees were instructed to leave their laptops in the office. (<https://www.esquire.com/news-politics/a49902/the-russian-amigre-leading-the-fight-to-protect-america/>)

Why does a cyber security company wait 45 days after allegedly uncovering a massive Russian attack on the DNC server to take concrete steps to safeguard the integrity of the information held on the server? This makes no sense.

A more plausible explanation is that it was discovered that emails had been downloaded from the server and copied onto a device like a thumbdrive. But the culprit had not yet been identified. We know one thing for certain--Crowdstrike did not take steps to shutdown and repair the DNC network until 10 days after the last email was copied from the server.

The final curiosity is that the DNC never provided the FBI access to its servers in order for qualified FBI technicians to conduct a thorough forensic examination. If this had been a genuine internet hack, it would be very easy for the NSA to identify when the information was taken and the route it moved after being hacked from the server. The NSA had the technical collection systems in place to enable analysts to know the date and time of the messages. But that has not been done.

Taken together, these disparate data points combine to paint a picture that exonerates alleged Russian hackers and implicates persons within our law enforcement and intelligence community taking part in a campaign of misinformation, deceit and incompetence. It is not a pretty picture.

On Feb 12, 2019, at 6:12 PM, Ty Dwenger <tydwenger@hush.com> wrote:

I think it's great. I highlighted a couple of words ("date" and "data") that may have been interchanged, but everything else looks great.

On Tuesday, February 12, 2019, 3:03:19 PM EST, Larry Johnson <ljohnson1@me.com> wrote:

Wanted to keep you guys updated on the piece that is in draft. Please read and let me know your thoughts.

The FBI, CIA and NSA claim that the DNC emails published by WIKILEAKS on July 26, 2016 were obtained via a Russian hack, but they have provided no forensic evidence to support that claim. An examination of the forensic evidence directly undermines the claim of the intelligence/law enforcement community and supports the hypothesis that the files taken from the DNC on the 25th of May 2016 were copied onto a file storage device, such as a thumb drive. If the Russians actually had conducted an internet based hack of the DNC computer network then the evidence of such an attack would have been collected and stored by the National Security Agency. The technical systems to accomplish this task have been in place since 2002. It is worth noting the tardy announcement that the DNC never with

the judgement in the January 2017 "Intelligence Community Assessment," regarding Russian interference in the 2016 Presidential election:

We also assess Putin and the Russian Government aspired to help President-elect Trump's election chances when possible, by discrediting Secretary Clinton and publicly contrasting her unfavorably to him. All three agencies agree with this judgment. CIA and FBI have high confidence in this judgment; NSA has moderate confidence.

In light of the established capability of the NSA to collect corroborating evidence for this particular judgment, the phrase, "moderate confidence" is a clear indicator that the NSA had not examined any of the emails from the alleged DNC "hack" and linked them to Russian agents. Had they done so, there would be no doubt about Russian culpability. And the NSA could make such a declaratory judgment in an unclassified assessment without compromising sources and methods. This is the equivalent of the dog that did not bark.

We believe that Special Counsel Robert Mueller faces major embarrassment if he decides to pursue the indictment he filed, which names 12 Russian GRU military personnel and a person identified as Guccifer 2.0, as the ones responsible for the DNC hack. According to a DOJ press release on the indictment, Mueller claims the emails were obtained via a "spearphishing" attack:

In 2016, officials in Unit 26165 began spearphishing volunteers and employees of the presidential campaign of Hillary Clinton, including the campaign's chairman. Through this process, officials in this unit were able to steal the usernames and passwords for numerous individuals and use those credentials to steal email content and hack into other computers. They also were able to hack into the computer networks of the Democratic Congressional Campaign Committee (DCCC) and the Democratic National Committee (DNC) through these spearphishing techniques to steal emails and documents, covertly monitor the computer activity of dozens of employees, and implant hundreds of files of malicious computer code to steal passwords and maintain access to those networks.

The officials in Unit 26165 coordinated with officials in Unit 74455 to plan the release of the stolen documents for the purpose of interfering with the 2016 presidential election. Defendants registered the domain DCLeaks.com and later staged the release of thousands of stolen emails and documents through that website. On the website, defendants claimed to be "American Hackers" and used Facebook accounts with fictitious names and Twitter accounts to promote the website. After public accusations that the Russian government was behind the hacking of DNC and DCCC computers, defendants created the fictitious persona Guccifer 2.0. On the evening of June 16, 2016 between 4:19PM and 4:56PM, defendants used their Moscow-based server to search for a series of English words and phrases that later appeared in Guccifer 2.0's first blog post falsely claiming to be a lone Romanian hacker responsible for the hacks in the hopes of undermining the allegations of Russian involvement.

(<https://www.justice.gov/eoir/grand-jury-indict-12-russian-intelligence-officers-hacking-officers-released-2016-election>)

Notwithstanding the DOJ press release, an examination of the Wikileaks DNC files do not support the claim that the emails were obtained via spearphishing. Instead, the evidence clearly shows that the emails posted on the Wikileaks site were copied onto an electronic media, such as a CD-ROM or thumbdrive before they were posted at Wikileaks.

We have examined the Wikileaks DNC files, which were actually created on 23, 25 and 26 May. In other words, those emails were copied on three different dates. Use of the FAT system indicates data transfer to a storage device, such as a thumb drive.

How do we know? The truth lies in the "last modified" time stamps on the Wikileaks files. Every single one of these time stamps end in even numbers. If you are not familiar with the FAT file system, you must understand that when data is stored under this system the data rounds the time to the nearest even numbered second.

We have examined 600 DNC email files stored on Wikileaks and all 600 files end in an even number—2, 4, 6, 8 or 0. If a system other than FAT had been used, there would have been an equal probability of the time stamp ending with an odd number. But that is not the case with the data stored on the Wikileaks site. All end with an even number.

The DNC emails are in 4 batches (times are GMT):

Date	Count	Min Time	Max Time	FAT	Min ID	Max ID
2016-05-23	10620	02:12:38	02:46:42	x	3800	14310
2016-05-25	11926	05:21:30	06:04:36	x	1	22458
2016-05-26	13357	14:11:36	20:06:04	y	22457	44055

The random probability that FAT was not used is 1 chance in 2 to the 500th power or approximately 1 chance in 10 to the 150th power - in other words, an infinitesimal of higher order.

This does not prove that the emails were copied at the DNC headquarters. But it does prove that the data/emails posted by Wikileaks did go through a storage device, like a thumbdrive, before Wikileaks posted the emails on the

World Wide Web.

If Mueller tries to bring this case against the 12 Russian soldiers to Court,

he will need to provide evidence that the storage device was not connected to the DNC local network. Otherwise, the defense will argue, and rightly so, that someone copied the DNC files to a storage device (e.g., USB thumb drive) and transferred that to WikiLeaks.

We also tested the hypothesis that WikiLeaks could have manipulated the files to produce the FAT result by comparing the DNC email files with the Podesta emails (aka Letter file) that was released on 21 September 2016. The FAT file format is NOT present in the Podesta files. If WikiLeaks employed a standard protocol for handling data/emails received from unknown sources then it would be sensible to conclude that the file structure of the DNC emails matched the file structure of the Podesta emails.

But the evidence shows otherwise.

Bill Binney, a former Technical Director of the National Security Agency, along with other former intelligence community experts, examined emails posted by Guccifer 2.0 and discovered that those emails could not have been downloaded over the Internet as a result of a spearphishing attack. It is a simple matter of mathematics and physics.

Shortly after WikiLeaks announced it had the DNC emails, Guccifer 2.0 emerged on the public stage, claiming that he hacked the DNC and that he had the DNC emails. Guccifer 2.0 began in late June 2016 to publish documents as proof that "he" had hacked from the DNC.

Taking Guccifer 2.0 at face value—i.e., that his documents were obtained via an Internet attack—Bill Binney conducted a forensic examination of the metadata contained in the posted documents based on Internet connection speeds in the United States. This analysis showed that the highest transfer rate was 48.1 megabytes per second, which is much faster than possible from a remote online connection.

Bill Binney and other colleagues with technical expertise extended the examination and ran various tests forensic from the Netherlands, Albania, Belgrade and the UK. The fastest rate obtained -- from a data center in New Jersey to a data center in the UK--was 12 megabytes per second, which is less than a fourth of the rate necessary to transfer the data, as it was listed from Guccifer 2.

The 48.1 megabytes speed coincides with the download rate for a thumb drive.

The findings from the examination of the Guccifer 2.0 data and the WikiLeaks data does not prove who was responsible for copying the information to a thumbdrive but it does refute the Special Counsel's claim that the DNC was hacked. It was not an Internet spearphishing attack. The data breach was local. It was copied from the network.

There is other circumstantial evidence that buttresses the conclusion that the data breach was a local effort that copied data.

First there is the Top Secret information leaked by Edward Snowden. If the DNC emails had been hacked via spearphishing (as alleged by Mueller), then the data would have been captured by the NSA by means of the Upstream program (Fairview, Stormcrow, Barney, Oakstar) and the forensic evidence would not modify files -- the data would be preserved as sent.

Second, we have the public reporting on the DNC and Crowdstrike, which provide a bizarre timeline for the alleged Russian hacking.

It was 29 April 2016, when the DNC claims it became aware its servers had been penetrated (see <https://medium.com/homafrost-riding/did-a-thunder-truck-hack-crowdstrike--conned-america-on-the-back-of-the-dnc-ecfa622f44ff>). No claim yet about who was responsible.

According to Crowdstrike founder, Dmitri Alperovitch, his company first detected the Russians mucking around inside the DNC server on 6 May 2016. A Crowdstrike Intelligence analyst reportedly told Alperovitch that:

Falcon had identified not one but two Russian intruders: Cozy Bear, a group Crowdstrike's experts believed was affiliated with the FSB, Russia's answer to the CIA, and Fancy Bear, which they had linked to the GRU, Russian military intelligence.

(<https://www.esquire.com/news-politics/a48903/the-russian-emigre-leading-the-fight-to-protect-america/>).

And what did Crowdstrike do about this? Nothing. According to Michael Isikoff, Crowdstrike claimed their inactivity was a deliberate plan to avoid alerting the Russians that they had been "discovered." This is nonsense. If you discovered a thief breaking into your house and you wait in the process of stealing its contents, what can you

Messages

enforcement officer would counsel doing nothing in order to avoid alerting the thief? Other nonsense.

We know from examining the WikiLeaks data that the last message copied from the DNC network is dated Wed, 25 May 2016 08:48:35. No emails were taken and released to WikiLeaks after that date.

CrowdStrike worked until 10 June 2016 to take concrete steps to clean up the DNC network. Apterovitch told Esquire's Vicky Ward that:

Ultimately, the teams decided it was necessary to replace the software on every computer at the DNC. Until the network was clean, secrecy was vital. On the afternoon of Friday, June 10, all DNC employees were instructed to leave their laptops in the office.

Apterovitch requires concrete details: <https://www.esquire.com/story/news/politics/russia-dnc-emails-origins-leading-the-fake-to-protect-america/1259482>

Why does a cyber security company wait 45 days after allegedly uncovering a massive Russian attack on the DNC server to take concrete steps to safeguard the integrity of the information held on the server? This makes no sense.

A more plausible explanation is that it was discovered that emails had been downloaded from the server and copied onto a device like a thumbdrive. But the culprit had not yet been identified. We know and thing for certain: Crowdstrike did not take steps to shut down and repair the DNC network until 15 days after the last email was copied from the server.

The final curiosity is that the DNC never provided the FBI access to its servers in order for qualified FBI technicians to conduct a thorough forensic examination. If this had been a genuine internet hack, it would be very easy for the NSA to identify when the information was taken and the route it moved after being hacked from the server. The NSA had the technical collection systems in place to enable analysts to know the date and time of the messages. But that has not been done.

Taken together, these disparate data points combine to paint a picture that exonerates alleged Russian hackers and implicates our law enforcement and intelligence community in a campaign of misinformation, deceit and

Sent to **Malia Zimmerman** on Mar 28, 2019 8:54:44 PM

<https://wikileaks.org/dnc-emails/>

Sent to **Malia Zimmerman** on Mar 28, 2019 8:54:44 PM

WikiLeaks - Search the DNC email database

Sent to **Malia Zimmerman** on Mar 28, 2019 8:56:30 PM

As instructions will vary from browser to browser, I figured I'd just explain how to get this through a third-party site that replicates and displays the HTTP response headers; however, if you would like browser-specific instructions just let me know what browser Larry is using and I'll write up a quick explanation.

If you visit <https://wcbniffer.co/?url=https://wikileaks.org/dnc-emails/gst/100...> then click submit, then scroll down to the "HTTP response headers" section you'll find the "Last-Modified" timestamp there. - Same thing for any other email, just switch out the 100 for whatever email ID you'd like to check.

Sent to **Ed Henry** on Mar 29, 2019 6:06:15 PM

This looks it ...
TEST IT YOURSELF, THE FAT FORMAT OF THE DNC EMAILS
By
William Binney
Adam Carter
Larry Johnson

Bill and I published a piece a few weeks back that provides actual evidence to debunk the claim that "Russia hacked the DNC." Yes, we know, the Mueller Report continues to insist that theft of emails from the DNC was done over the Internet. But that conclusion rests on the opinion of third parties who offer no actual forensic evidence. We, by contrast, are offering up actual evidence. Do not take our word for it. You can test it yourself. We are going to show you how.

First, let's review our key findings from the original piece:

An examination of the WikiLeaks DNC files shows they were created on 23, 25 and 30 May respectively. The fact that they appear in a FAT system format indicates the data was transferred to a storage device, such as a thumb drive.

How do we know? The truth lies in the "last modified" time stamps on the WikiLeaks files. Every single one of those time stamps end in even numbers. If you are not familiar with the FAT file system, you need to understand that when a date is stored under this system the data rounds the time to the nearest even numbered second.

Messages

We have examined 500 DNC emails (see stored on WikiLeaks and 500 have ended in an even number—2, 4, 6, 8 or 0. If a system other than FAT had been used, there would have been an equal probability of the time stamp ending with an odd number. But that is not the case with the data stored on the WikiLeaks site. All end with an even number.

Here's what you need to do to replicate what we found:

Step One—Go to the WikiLeaks DNC email database. Click here: <https://wikileaks.org/dnc-emails/>

Step Two—Search the DNC database using the word Clinton. This will produce the following results. (see link https://wikileaks.org/dnc-emails/?q=Clinton&from=&to=&file=¬e=&date_from=&date_to=&nafrom=¬e=&count=50&sort=0&searchresult)

The first message in terms of "relevance" is
Doc ID

Date

Subject

From

To

To:

2016-05-23 2:17:56 +0000

POLITICO's 2016 Blast: Bernie's DNC concessions — Hillary Clinton's fall preparations — Trump and Clinton get personal again — 5 Things You Need To Know

2016blast@politico.com

Kaplan@DNC.org

Step Three—Go to the webfilter site and direct it to "get/100". This is computer speak telling the program to find message 100 (which is titled POLITICO's 2016 Blast: Bernie's DNC concessions — Hillary Clinton's fall preparations — Trump and Clinton get personal again — 5 Things You Need To Know." <https://webfilter.cc?url=https://wikileaks.org/dnc-emails/get/100> ...

Step Four—Click on submit. That will take you to the following document:

Step Five—Scroll down to the "HTTP response headers" section where you will find the "Last-Modified" timestamp.

Message 100 shows a Last Modified Timestamp of 05:22:40 GMT.

That time equates to 01:22:40 Eastern Daylight Time.

It ends in 0, an even number. Our search and analysis of all the messages from the DNC show that all end in an even number.

We repeat our conclusion from the original article:

The random probability that FAT was not used is 1 chance in 2 to the 500th power or approximately 1 chance in 10 to the 150th power – in other words, an infinitely high odds.

This data alone does not prove that the emails were copied at the DNC headquarters. But it does show that the data/emails posted by WikiLeaks did go through a storage device, like a thumbdrive, before WikiLeaks posted the emails on the World Wide Web.

Who was the person or persons at the DNC that were copying these messages to a storage device, like a thumb drive, early in the morning on Wednesday the 25th of May? We have an opinion, but our focus is not on speculation. Let us first deal with the hard forensic evidence. These emails were not "hacked" in a spearphishing attack. They were taken by someone who had direct access to the DNC servers and someone who copied the messages onto a physical storage device. This is the FAT truth.

Sent to Arthur Schwartz on Mar 30, 2019 11:45:27 AM

WHY THE DNC WAS NOT HACKED BY THE RUSSIANS
By
William Binney
Larry Johnson

The FBI, CIA and NSA claim that the DNC emails published by WIKILEAKS on July 26, 2016 were obtained via a Russian hack, but more than three years after the alleged "hack" no forensic evidence has been produced to support that claim. In fact, the available forensic evidence contradicts the official account that blames the leak of the DNC emails on a Russian internet "intrusion". The existing evidence supports an alternative explanation – the files taken from the DNC on between 23 and 26 May 2016 and were copied onto a file storage device, such as a thumb drive.

If the Russians actually had conducted an Internet based hack of the DNC computer network then the evidence of such an attack would have been collected and stored by the National Security Agency. The technical systems to accomplish this task have been in place since 2002. The NSA had an opportunity to make it clear that there was irrefutable proof of Russian meddling, particularly with regard to the DNC hack, when it signed on to the January 2017 Intelligence Community Assessment (ICA) that Russian intelligence had hacked the DNC. Such a statement would

Intelligence Community Assessment, "regarding Russian interference in the 2016 Presidential Election."

We also assess Putin and the Russian Government aspired to help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him. All three agencies agree with this judgment. CIA and FBI have high confidence in this judgment; NSA has moderate confidence.

The phrase, "moderate confidence" is intelligence speak for "we have no hard evidence." Thanks to the leaks by Edward Snowden, we know with certainty that the NSA had the capability to examine and analyze the DNC emails. NSA routinely "vacuumed up" email traffic transiting the U.S., using robust collection systems (whether or not anyone in the NSA chose to look for this data is another question). If those emails had been hacked over the internet then NSA also would have been able to track the electronic path they traveled over the internet. This kind of data would allow the NSA to declare without reservation or caveat that the Russians were guilty. The NSA could admit to such a fact in an unclassified assessment without compromising sources and methods. Instead, the NSA only claimed to have moderate confidence in the judgment regarding Russian meddling. If the NSA had hard intelligence to support the judgment the conclusion would have been stated as "full confidence."

We believe that Special Counsel Robert Mueller faces major embarrassment if he decides to pursue the indictment he filed—which accuses 12 Russian GRU military personnel and an entity identified as, Guccifer 2.0, for the DNC hack—because the available forensic evidence indicates the emails were copied onto a storage device.

According to a DOJ press release on the indictment of the Russians, Mueller declares that the emails were obtained via a "spearphishing" attack:

In 2016, officials in Unit 26165 began spearphishing volunteers and employees of the presidential campaign of Hillary Clinton, including the campaign's chairman. Through this process, officials in this unit were able to steal the usernames and passwords for numerous individuals and use those credentials to steal email content and hack into other computers. They also were able to hack into the computer networks of the Democratic Congressional Campaign Committee (DCCC) and the Democratic National Committee (DNC) through these spearphishing techniques to steal emails and documents, covertly monitor the computer activity of dozens of employees, and implant hundreds of files of malicious computer code to steal passwords and maintain access to these networks.

The officials in Unit 26165 coordinated with officials in Unit 34455 to plan the release of the stolen documents for the purpose of interfering with the 2016 presidential election. Defendants registered the domain DCLinks.com and later stored the release of thousands of stolen emails and documents through that website. On the website, defendants claimed to be "American hackers" and used Facebook accounts with fictitious names and Twitter accounts to promote the website. After public accusations that the Russian government was behind the hacking of DNC and DCCC computers, defendants created the fictitious persona Guccifer 2.0. On the evening of June 16, 2016 between 4:19PM and 4:56PM, defendants used their Moscow-based server to search for a series of English words and phrases that later appeared in Guccifer 2.0's first blog post falsely claiming to be a lone Romanian hacker responsible for the hacks in the hopes of undermining the allegations of Russian involvement.

<https://www.justice.gov/opa/pr/indict-12-russian-intelligence-officers-hacking-offices-related-2018-election>

Notwithstanding the DOJ press release, an examination of the WikiLeaks DNC files do not support the claim that the emails were obtained via spearphishing. Instead, the evidence clearly shows that the emails posted on the WikiLeaks site were copied onto an electronic media, such as a CD-ROM or thumbdrive before they were posted at WikiLeaks. The emails posted on WikiLeaks were saved using the File Allocation Table (aka FAT) computer file system architecture.

An examination of the WikiLeaks DNC files shows they were created on 23, 26 and 28 May respectively. The fact that they appear in a FAT system format indicates the data was transferred to a storage device, such as a thumb drive.

How do we know? The truth lies in the "last modified" time stamps on the WikiLeaks files. Every single one of these time stamps end in even numbers. If you are not familiar with the FAT file system, you need to understand that when a date is stored under this system the date rounds the time to the nearest even numbered second.

We have examined 500 DNC email files stored on WikiLeaks and all 500 files end in an even number—2, 4, 6, 8 or 0. If a system other than FAT had been used, there would have been an equal probability of the time stamp ending with an odd number. But that is not the case with the data stored on the WikiLeaks site. All end with an even number.

The DNC emails are in 3 batches (times are GMT).

Date	Count	Min Time	Max Time	FAT	Min Id	Max Id
2016-05-23	10620	02:12:38	02:46:42 x	3800	14318	
2016-05-26	11936	05:21:38	06:04:36 x	1	22456	
2016-05-26	13357	14:11:38	20:06:04 x	22457	44053	

The random probability that FAT was not used by 1 chance in 2 to the 500th power or approximately 1 chance in 10 to the 150th power—in other words, an infinitely high order.

This data alone does not prove that the emails were copied at the DNC headquarters. But it does show that the data emails posted by WikiLeaks did go through a storage device, like a thumbdrive, before WikiLeaks posted the emails on the World Wide Web.

This fact alone is enough to raise reasonable doubts about Mueller's indictment accusing 12 Russian soldiers as the suspects for the leak of the DNC emails to WikiLeaks. A savvy defense attorney will argue, and rightly so, that someone copied the DNC files to a storage device (E.g., USB thumb drive) and transferred that to WikiLeaks.

We also tested the hypothesis that WikiLeaks could have manipulated the files to produce the FAT result by comparing the DNC email files with the Podesta emails (aka Letter file) that was released on 21 September 2016. The FAT file format is NOT present in the Podesta files. If WikiLeaks employed a standard protocol for handling data/emails received from unknown sources we should expect the file structure of the DNC emails to match the file structure of the Podesta emails. The evidence shows otherwise.

There is further compelling technical evidence that undermines the claim that the DNC emails were downloaded over the internet as a result of a spearphishing attack. Bill Binney, a former Technical Director of the National Security Agency, along with other former intelligence community experts, examined emails posted by Guccifer 2.0 and discovered that those emails could not have been downloaded over the internet as a result of a spearphishing attack. It is a simple matter of mathematics and physics.

Shortly after Wikileaks announced it had the DNC emails, Guccifer 2.0 emerged on the public stage, claiming that "he" hacked the DNC and that he had the DNC emails. Guccifer 2.0 began in late June 2016 to publish documents as proof that "he" had hacked from the DNC.

Taking Guccifer 2.0 at face value—i.e., that his documents were obtained via an Internet attack—Bill Binney conducted a forensic examination of the metadata contained in the posted documents based on Internet connection speeds in the United States. This analysis showed that the highest transfer rate was 49.1 megabytes per second, which is much faster than possible from a remote online connection. The 49.1 megabytes speed coincides with the download rate for a thumb drive.

Binney, assisted by other colleagues with technical expertise, extended the examination and ran various tests forensic from the Netherlands, Albania, Belgrade and the UK. The fastest rate obtained -- from a data center in New Jersey to a data center in the UK--was 12 megabytes per second, which is less than a fourth of the rate necessary to transfer the data, as it was listed from Guccifer 2.

The findings from the examination of the Guccifer 2.0 data and the Wikileaks data does not prove who copied the information to a thumbdrive, but it does provide an empirical alternative explanation that undermines the Special Counsel's claim that the DNC was hacked. According to the forensic evidence for the Guccifer 2.0 data, the DNC emails were not taken by an Internet spearphishing attack. The data breach was local. It was copied from the network.

There is other circumstantial evidence that buttresses the conclusion that the data breach was a local effort that copied data.

First there is the Top Secret Information leaked by Edward Snowden. If the DNC emails had been hacked via spearphishing (as alleged by Mueller), then the data would have been captured by the NSA by means of the Upstream program (Falcon, Stomberg, Barney, Dakota) and the forensic evidence would not modify (since - the data would be processed as sent).

Second, we have the public reporting on the DNC and Crowdstrike, which provides a bizarre timeline for the alleged Russian hacking.

It was 29 April 2016, when the DNC claims it became aware its services had been penetrated (see <https://medium.com/homefront-raising/dumbstruck-how-crowdstrike-conned-america-on-the-back-of-the-dnc-2016-02f8441>). No claim yet about who was responsible.

According to Crowdstrike founder, Dmitri Alperovitch, his company first detected the Russians mucking around inside the DNC server on 6 May 2016. A Crowdstrike intelligence analyst reportedly told Alperovitch that:

Falcon had identified not one but two Russian intruders: Cozy Bear, a group Crowdstrike's experts believed was affiliated with the FSB, Russia's answer to the CIA; and Fancy Bear, which they had linked to the GRU, Russian military intelligence.

<https://www.esquire.com/news-politics/a49002/the-russian-emigre-leading-the-fight-to-protect-america/>

And what did Crowdstrike do about this? Nothing. According to Michael Isikoff, Crowdstrike claimed their inactivity was a deliberate plan to avoid alerting the Russians that they had been "discovered." This is nonsense. If a security company detected a thief breaking into a house and stealing its contents, what sane company would counsel the client to do nothing in order to avoid alerting the thief? Utter nonsense.

We know from examining the Wikileaks data that the last message copied from the DNC network is dated Wed, 26 May 2016 22:46:35. No DNC emails were taken and released to Wikileaks after that date.

Crowdstrike waited until 10 June 2016 to take concrete steps to clean up the DNC network. Alperovitch told Esquire's Vicky Ward that:

Ultimately, the teams decided it was necessary to replace the software on every computer at the DNC. Until the network was clean, secrecy was vital. On the afternoon of Friday, June 10, all DNC employees were instructed to leave their laptops in the office.

<https://www.esquire.com/news-politics/a49002/the-russian-emigre-leading-the-fight-to-protect-america/>

Why does a cyber security company wait 45 days after allegedly uncovering a massive Russian attack on the DNC server to take concrete steps to safeguard the integrity of the information held on the server? This makes no sense.

A more plausible explanation is that it was discovered that emails had been downloaded from the server and copied onto a device like a thumbdrive. But the culprit had not yet been identified. We know one thing for certain—Crowdstrike did not take steps to shutdown and repair the DNC network until 18 days after the last email was copied from the server.

The final reality is that the DNC never provided the FBI access to its servers in order for a qualified FBI technician to conduct a thorough forensic examination. If this had been a genuine Internet hack, it would be very easy for the NSA to identify when the information was taken and the route it moved after being hacked from the server. The NSA had the technical collection systems in place to enable analysts to know the date and time of the messages. But that has not been done.

Taken together, these disparate data points combine to paint a picture that exonerates alleged Russian hackers and implicates persons within our law enforcement and intelligence community taking part in a campaign of

Messages

mainstream, deceit and incompetence. It is not a pretty picture.

On Feb. 12, 2019, at 6:12 PM, Ty Cleveland <tycleveland@yahoo.com> wrote:

I think it's great. I highlighted a couple of words ("date" and "data") that may have been interchanged, but everything else looks great.

On Tuesday, February 12, 2019, 3:00:10 PM EST, Larry Johnson <ljohnson10@aol.com> wrote:

Wanted to keep you guys updated on the piece that is in draft. Please read and let me know your thoughts.

The FBI, CIA and NSA claim that the DNC emails published by WIKILEAKS on July 28, 2018 were obtained via a Russian hack, but they have provided no forensic evidence to support their claim. An examination of the forensic evidence clearly undermines the claim of the intelligence law enforcement community and supports the hypothesis that the files came from the DNC on the 25th of May 2018 were copied onto a file storage device, such as a thumb drive. If the Russians actually had conducted an internet based hack of the DNC computer network then the evidence of such an attack would have been collected and stored by the National Security Agency. The technical systems to accomplish this task have been in place since 2002. It is worth noting the tepid endorsement that the NSA gave with the judgement in the January 2017 "Intelligence Community Assessment," regarding Russian interference in the 2016 Presidential election:

We also assess Putin and the Russian Government aspire to help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him. All three agencies agree with this judgment. CIA and FBI have high confidence in this judgment; NSA has moderate confidence.

In light of the established capability of the NSA to collect corroborating evidence for this particular judgment, the phrase, "moderate confidence" is a clear indicator that the NSA had not examined any of the emails from the alleged DNC "hack" and linked them to Russian agents. Had they done so, there would be no doubt about Russian culpability. And the NSA could make such a declaratory judgment in an unclassified assessment without compromising sources and methods. This is the equivalent of the dog that did not bark.

We believe that Special Counsel Robert Mueller faces major embarrassment if he decides to pursue the indictment he filed, which names 12 Russian GRU military personnel and a person identified as, Guccifer 2.0, as the ones responsible for the DNC hack. According to a DOJ press release on the indictment, Mueller claims the emails were obtained via a "spearphishing" attack.

In 2016, officials in Unit 26166 began spearphishing volunteers and employees of the presidential campaign of Hillary Clinton, including the campaign chairman. Through that process, officials in this unit were able to steal the usernames and passwords for numerous individuals and use those credentials to steal email content and hack into other computers. They also were able to hack into the computer networks of the Democratic Congressional Campaign Committee (DCCC) and the Democratic National Committee (DNC) through these spearphishing techniques to steal emails and documents, covertly monitor the computer activity of dozens of employees, and implant hundreds of files of malicious computer code to steal passwords and maintain access to these networks.

The officials in Unit 26166 cooperated with officials in Unit 14455 to plan the release of the stolen documents for the purpose of interfering with the 2016 presidential election. Defendants registered the domain DCLeaks.com and later staged the release of thousands of stolen emails and documents through that website. On the website, defendants claimed to be "American hacktivists" and used Facebook accounts with fictitious names and Twitter accounts to promote the website. After public accusations that the Russian government was behind the hacking of DNC and DCCC computers, defendants created the fictitious persona Guccifer 2.0. On the evening of June 15, 2018 between 4:19PM and 4:26PM, defendants used their Moscow-based server to search for a series of English words and phrases that later appeared in Guccifer 2.0's first blog post falsely claiming to be a lone Romanian hacker responsible for the hacks in the hopes of undermining the allegations of Russian involvement.

<https://www.justice.gov/opa/pr/indict-12-russian-intelligence-officers-hacking-offenses-related-2016-election>

Notwithstanding the DOJ press release, an examination of the Wikileaks DNC files do not support the claim that the emails were obtained via spearphishing. Instead, the evidence clearly shows that the emails posted on the Wikileaks site were copied onto an electronic media, such as a CD-ROM or thumbdrive before they were posted at Wikileaks.

We have examined the Wikileaks DNC files, which were actually created on 23, 25 and 26 May. In other words, those emails were copied on three different dates. Use of the FAT system indicates data transfer to a storage device, such as a thumb drive.

How do we know? The truth lies in the "last modified" date stamps on the Wikileaks files. Every single one of these time stamps end in even numbers. If you are not familiar with the FAT file system, you must understand that when data is stored under this system, the date rounds the time to the nearest even-numbered second.

We have examined 500 DNC email files stored on Wikileaks and all 500 files end in an even number—2, 4, 6, 8 or 0. If a system other than FAT had been used, there would have been an equal probability of the time stamp ending with an odd number. But that is not the case with the data stored on the Wikileaks site. All end with an even number.

Messages

The DNC emails are in 4 batches (times are GMT).

Date	Count	Min Time	Max Time	FAT Min Id	Max Id
2016-06-23 10520	02-12:38	02-45:42 x	3800	14370	
2016-06-25 11935	05-21:30	05-04:39 x	1	23458	
2016-06-26 13357	14-11:36	20-08:04 x	22467	44089	

The random probability that FAT was not used is 1 chance in 2 to the 500th power or approximately 1 chance in 10 to the 150th power – in other words, an infinitesimal of higher order.

This does not prove that the emails were copied at the DNC headquarters. But it does prove that the data/emails posted by Wikileaks did go through a storage device, like a thumbdrive, before Wikileaks posted the emails on the World Wide Web.

If Mueller tries to bring this case against the 12 Russian soldiers to Court,

he will need to provide evidence that the storage device was not connected to the DNC local network. Otherwise, the defense will argue, and rightly so, that someone copied the DNC files to a storage device (Eg., USB thumb drive) and transferred that to Wikileaks.

We also tested the hypothesis that Wikileaks could have manipulated the files to produce the FAT result by comparing the DNC email files with the Podesta emails (aka Carter files) that was released on 21 September 2016. The FAT file format is NOT present in the Podesta files. If Wikileaks employed a standard protocol for handling data/emails received from unknown sources then it would be sensible to conclude that the file structure of the DNC emails matched the file structure of the Podesta emails.

But the evidence shows otherwise.

Bill Binney, a former Technical Director of the National Security Agency, along with other former intelligence community experts, examined emails posted by Guccifer 2.0 and discovered that those emails could not have been downloaded over the internet as a result of a spearphishing attack. It is a simple matter of mathematics and physics.

Shortly after Wikileaks announced it had the DNC emails, Guccifer 2.0 emerged on the public stage, claiming that he hacked the DNC and that he had the DNC emails. Guccifer 2.0 began in late June 2016 to publish documents as proof that "he" had hacked from the DNC.

Taking Guccifer 2.0 at face value – i.e., that his documents were obtained via an internet attack – Bill Binney conducted a forensic examination of the metadata contained in the posted documents based on internet connection speeds in the United States. This analysis showed that the highest transfer rate was 48.1 megabytes per second, which is much faster than possible from a remote online connection.

Bill Binney and other colleagues with technical expertise defended the examination and ran various tests forensic from the Netherlands, Albania, Bangladesh and the UK. The fastest rate obtained -- from a data center in New Jersey to a data center in the UK -- was 12 megabytes per second, which is less than a fourth of the rate necessary to transfer the data, as it was listed from Guccifer 2.

The 48.1 megabytes speed coincides with the download rate for a thumb drive.

The findings from the examination of the Guccifer 2.0 data and the Wikileaks data does not prove who was responsible for copying the information to a thumbdrive but it does refute the Special Counsel's claim that the DNC was hacked. It was not an internet spearphishing attack. The data breach was local. It was copied from the network.

There is other circumstantial evidence that buttresses the conclusion that the data breach was a local effort that copied data.

First there is the Top Secret information leaked by Edward Snowden. If the DNC emails had been hacked via spearphishing (as alleged by Mueller) then the data would have been captured by the NSA by means of the upstream program (Fairview, Stormbrew, Beamix, Oakstar) and the forensic evidence would not modify times – the data would be presented as sent.

Second, we have the public reporting on the DNC and Obamas' strike, which provides a bizarre timeline for the alleged Russian hacking.

Messages

It was 29 April 2016, when the DNC claims it became aware its servers had been penetrated (see <https://medium.com/homefront-rising/dumbest-truck-horn-crowdstrike-conned-america-on-the-back-of-the-dnc-e6fa522f44f1>). No claim yet about who was responsible.

According to CrowdStrike founder, Dmitri Alperovitch, his company first detected the Russians mucking around inside the DNC server on 6 May 2016. A CrowdStrike intelligence analyst reportedly told Alperovitch that:

Falcon had identified not one but two Russian intruders: Cozy Bear, a group CrowdStrike's experts believed was affiliated with the FSB, Russia's answer to the CIA; and Fancy Bear, which they had linked to the GRU, Russian military intelligence.

(<https://www.esquire.com/news-politics/a48902/the-russian-smigra-leading-the-fight-to-protect-america/>)

And what did CrowdStrike do about this? Nothing. According to Michael Iskeff, CrowdStrike claimed their inactivity was a deliberate plan to avoid alerting the Russians that they had been "discovered." This is nonsense. If you discovered a thief breaking into your house and who was in the process of stealing its contents, what sane law enforcement officer would counsel doing nothing in order to avoid alerting the thief? Utter nonsense.

We know from examining the Wikileaks data that the last message copied from the DNC network is dated Wed, 26 May 2016 20:45:39. No emails were taken and released to Wikileaks after that date.

CrowdStrike waited until 10 June 2016 to take concrete steps to clean up the DNC network. Alperovitch told Esquire's Vicky Ward that:

Ultimately, the teams decided it was necessary to replace the software on every computer at the DNC. Until the network was clean, secrecy was vital. On the afternoon of Friday, June 10, all DNC employees were instructed to leave their laptops in the office.

(<https://www.esquire.com/news-politics/a48902/the-russian-smigra-leading-the-fight-to-protect-america/>)

Why does a cyber security company wait 45 days after allegedly uncovering a massive Russian attack on the DNC server to take concrete steps to safeguard the integrity of the information held on the server? This makes no sense.

A more plausible explanation is that it was discovered that emails had been downloaded from the server and copied onto a device like a thumb drive. But the culprit had not yet been identified. We know one thing for certain—CrowdStrike did not take steps to shutdown and repair the DNC network until 10 days after the last email was copied from the server.

The final curiosity is that the DNC never provided the FBI access to its servers in order for qualified FBI technicians to conduct a thorough forensic examination. If this had been a genuine internet hack, it would be very easy for the FBI to identify when the information was taken and the route it moved after being hacked from the server. The NSA had the technical collection systems in place to enable analysts to know the date and time of the messages. But that had not been done.

Taken together, these disparate data points combine to paint a picture that exonerates alleged Russian hackers and implicates our law enforcement and intelligence community in a campaign of misinformation, deceit and



Sent to Arthur Schwartz on Mar 30, 2019 11:45:45 AM

This is a link to
TEST IT YOURSELF, THE FAT FORMAT OF THE DNC EMAILS

By
William Binney
Adam Carter
Larry Johnson

Bill and I published a piece a few weeks back that provides actual evidence to debunk the claim that "Russia hacked the DNC." Yes, we know, the Mueller Report continues to insist that theft of emails from the DNC was done over the Internet. But that conclusion rests on the opinion of third parties who offer no actual forensic evidence. We, by contrast, are offering up actual evidence. Do not take our word for it. You can test it yourself. We are going to show you how.

First, let's review our key findings from the original piece:

An examination of the Wikileaks DNC files shows they were created on 23, 25 and 26 May respectively. The fact that they appear in a FAT system format indicates the data was transferred to a storage device, such as a thumb drive.

How do we know? The truth lies in the "last modified" time stamps on the Wikileaks files. Every single one of these time stamps end in even numbers. If you are not familiar with the FAT file system, you need to understand that when a date is stored under this system the date rounds the time to the nearest even numbered second.

(If you are familiar with FAT file systems, you will know that the time is stored in a 28-bit field, which means it can only represent times from 0 to 65,535 seconds, or 18 hours, 15 minutes, and 45 seconds.)

Messages

We have examined our own logs, email lists stored on Wikileaks servers and did not find an even number — 2, 4, 6, 8 or 10 — a system other than FAT had been used, there would have been an equal probability of the time stamp ending with an odd number. But that is not the case with the data stored on the Wikileaks site. All end with an even number.

Here's what you need to do to replicate what we found:

Step One—Go to the Wikileaks DNC email database. Click here: <https://wikileaks.org/dnc-emails>

Step Two—Search the DNC database using the word Clinton.
This will produce the following results (see link https://wikileaks.org/dnc-emails?q=Clinton&from=&to=&title=&date_from=&date_to=&refrom=¬e=&count=50&sort=0#selectresult)

The first message in terms of "relevance" is
Doc ID

Date

Subject

From

To

100
2016-05-24 1:17:55 -0400
POLITICO's 2016 Blast: Bernie's DNC concessions — Hillary Clinton's fall preparations — Trump and Clinton get personal again — 6 Things You Need To Know
2016blast@politica.com
kaplan@dncc.org

Step Three—Go to the webfilter site and direct it to "100/100". This is computer speak telling the program to find message 100 (which is titled POLITICO's 2016 Blast: Bernie's DNC concessions — Hillary Clinton's fall preparations — Trump and Clinton get personal again — 6 Things You Need To Know." <https://webfilterfor.com?url=https://wikileaks.org/dnc-emails/get/100> ...

Step Four—Click on submit. That will take you to the following document:

Step Five—scroll down to the "HTTP response headers" section where you will find the "Last-Modified" timestamp.

Message 100 shows a Last-Modified Timestamp of 05:22:00 GMT.

That time equates to 01:22:00 Eastern Daylight Time.

It ends in 0, an even number. Our search and analysis of all the messages from the DNC show that all end in an even number.

We repeat our conclusion from the original article:

The random probability that FAT was not used is 1 chance in 2 to the 500th power or approximately 1 chance in 10 to the 150th power — in other words, an infinitely high order.

This data alone does not prove that the emails were copied at the DNC headquarters. But it does show that the data/emails posted by Wikileaks did go through a storage device, like a thumbdrive, before Wikileaks posted the emails on the World Wide Web.

Who was the person or persons at the DNC that were copying these messages on a storage device, like a thumb drive, early in the morning on Wednesday the 26th of May? We have an opinion, but our focus is not on speculation. Let us first deal with the hard forensic evidence. These emails were not "hacked" in a spearphishing attack. They were taken by someone who had direct access to the DNC servers and someone who copied the messages onto a physical storage device. This is the FAT truth.

Received from **Cassandra Fairbanks** on Apr 21, 2019 4:47:30 AM

CF

Wikileaks just tweeted right now, nothing unusual

Received from **Malia Zimmerman** on Apr 23, 2019 8:55:05 PM

MZ

<https://www.rollingstone.com/politics/politics-news/wikileaks-and-fox-news-are-silent-on-the-debunked-seth-rich-conspiracy-theory-825686/>

Messages

Sent to +19727683560 on Oct 7, 2019 10:02:42 PM

Ed Butowsky will be speaking about how he became the center piece of the Trump, Wikileaks, Seth Rich, and Russia controversy. He will also discuss how he was involved in creating the back 13 Hours and how he was instrumental in putting together the Benghazi select committee. This will be one of the first time that has spoken publicly about his involvement in both of these major national news stories.

Ed is a prominent wealth manager based in Plano, Texas. For the past 30 years he has managed money for some of the wealthiest people in the world including celebrities and professional athletes.

Ed Butowsky frequently appears on all the television outlets including Fox News, FOXBusiness and CNBC.



Received from +14012346757 on Nov 12, 2019 6:17:36 PM



Richard Gates, who is facing up to ten years in prison under a plea agreement for various fraud charges, testified in Stone's criminal trial on Tuesday, saying that the longtime Trump associate was telling the campaign about WikiLeaks's plans as early as April 2016, months before the DNC had announced it was hacked.

Sent to Greg Peters on Mar 11, 2020 5:07:22 PM

10 MARCH 2020

Did Joe Biden's former IT Guy Masquerade as Guccifer 2.0? by Larry E. Johnson

Why does the name of Joe Biden's former internet technology guru, Warren Flood, appear in the meta data of documents posted on the internet by Guccifer 2.0? In case you do not recall, Guccifer 2.0 was identified as someone tied to Russian intelligence who played a direct role in creating emails from John Podesta. The meta data in question indicates the name of the person who actually copied the original document. We have this irrefutable fact in the documents unveiled by Guccifer 2.0--Warren Flood's name appears prominently in the meta data of several documents attributed to "Guccifer 2.0." When this transpired, Flood was working as the CEO of his own company, BRIGHT BLUE DATA, (brightbluedata.com). Was Flood tasked to masquerade as a Russian operative?

Gave Flood some props if that is true--he fooled our Intelligence Community and the entire team of Mueller prosecutors into believing that Guccifer was part of a Russian military intelligence cyber attack. But a careful examination of the documents shows that it is highly unlikely that this was an official Russian cyber operation.

Here's what the U.S. Intelligence Community wrote about Guccifer 2.0 in their very flawed January 2017 Intelligence Community Assessment:

We assess with high confidence that the GRU used the Guccifer 2.0 persona, DCLeaks.com, and Wikileaks to release US victim data obtained in cyber operations publicly and in exclusives to media outlets.

Guccifer 2.0, who claimed to be an independent Romanian hacker, made multiple contradictory statements and false claims about his likely Russian identity throughout the election. Press reporting suggests more than one person claiming to be Guccifer 2.0 interacted with journalists.

Content that we assess was taken from e-mail accounts targeted by the GRU in March 2016 appeared on DCLeaks.com starting in June.

The basis of the intelligence Community in dealing with circumstantial evidence was marred by a disturbing lack of candor on the part of the Mueller investigators and prosecutors. Here's the full tale they spun about Guccifer 2.0.

On June 14, 2016, the DNC and its cyber-response team announced the breach of the DNC network and suspected theft of DNC documents. In the statements, the cyber-response team alleged that Russian state-sponsored actors (which they referred to as "Fancy Bear") were responsible for the breach. Apparently in response to that announcement, on June 15, 2016, GRU officers using the persona Guccifer 2.0 created a WordPress blog. In the hours leading up to the launch of that WordPress blog, GRU officers logged into a Moscow-based server used and managed by Unit 74455 and searched for a number of specific words and phrases in English, including "hundreds of deaths," "Islamist," and "Northside known." Approximately two hours after the last of those searches, Guccifer 2.0 published its first post, attributing the DNC server hack to a lone Romanian hacker and using several of the unique English words and phrases that the GRU officers had searched for that day.

The claims by both the Intelligence Community and the Mueller team about Guccifer 2.0 are an astounding, incredible denial of critical evidence pointing to a U.S. actor, not a Russian or Romanian. No one in this "august" group took the time to examine the metadata on the documents posted by "Guccifer 2.0" to his website on June 15, 2016.

I wish I could claim credit for the following forensic analyses, but the honors are due to Yacov Appelbaum. While there are many documents in the Podesta haul that match the following pattern, this analysis focuses only on a document originally created by the DNC's Director of Research, Lauren Dillon. This document is the Trump Opposition Report document.

According to Appelbaum, the Trump Opposition Report document, which was "published" by Guccifer 2.0, shows clear evidence of digital manipulation:

A US based user (hereafter referred to as G2) operating initially from the West coast and then, subsequently, from the East coast, changes the MS Word 2007 and Operating System language settings to Russian.

G2 opens and saves a document with the file name, "12102015 Trump Report - for dist-4.docx". The document bears the title, "Donald Trump Report" (which was originally composed by Lauren Dillon aka DILLON REPORT) as an RTF file and opens it again.

G2 opens a second document that was attached to an email sent on December 21, 2008 to John Podesta, from Sara Latham Spett gav. This WORD document lists prospective nominees for posts in the Department of Agriculture for the upcoming Obama Administration. It was generated by User--Warren Flood--on a computer registered to the General Services Administration (aka GSA) named "Susan J. Domestile - USDA - 2008-12-20-3.doc", which was kept

by Podesta on his private Gmail account. I refer to this as the "WARREN DOCUMENT" in this analysis.

G2 deleted the content of the 2008 Warren Document and saves the empty file as a RTF, and opens it again.

G2 copies the content of the "Dillon Report" (which is an RTF document) and pastes it into the 2008 Warren Document template, i.e. the empty RTF document.

G2 user makes several modifications to the content of this document. For example, the Warren Document contained the watermark "CONFIDENTIAL DRAFT". G2 deleted the word "DRAFT" but kept the "CONFIDENTIAL" watermark.

G2 saves this document into a file called "1.doc". This document now contains the text of the original Lauren Dillon "Donald Trump Report" document, but also contains Russian language UML links that generate error messages.

G2's 1.DOC (the Word version of the document) shows the following meta data attributes:

Created at 6/15/2016 at 1:39pm by "WARREN FLOOD"

Last Modified at 6/15/2016 at 1:45pm by "Феликс Эдмундович" (Felix Edmundovich, the first and middle name of Dzerzhinsky, the creator of the predecessor of the KGB. It is assumed the Felix Edmundovich refers to Dzerzhinsky.)

G2 also produces a pdf version of this document almost four hours later. It is created at 6/15/2016 at 5:04:16pm by "WARREN FLOOD."

G2 first publishes "1.doc" to various media outlets and then uploads a copy to the Quodlibet 2.0 WordPress website (which is hosted in the United States).

There are several critical facts from the metadata that destroy the claim that Quodlibet 2.0 was a Romanian or a Russian.

The computer used to create the original Warren Document (dated 2008) was a US Government computer issued to the Obama Presidential Transition Team by the General Services Administration.

The Warren Document and the 1.DOC were created in the United States using Microsoft Word software (2007) that is registered to the GSA.

The author of both 1.doc and the PDF version is identified as "WARREN FLOOD."

The copy of "1.doc" was uploaded on a server located in the United States.

"Russian" fingerprints were deliberately inserted into the text and the meta data of "1.doc."

This begs a very important question: Did Warren Flood actually create these documents or was someone masquerading as Warren Flood? Unfortunately, neither the Intelligence Community nor the Mueller Special Counsel investigators provided any evidence to show they examined this forensic data. More troubling is the fact that the Microsoft Word processing software being used is listed as a GSA product.

Trump-apps-versions-metadata_thumb-1

If this was truly a Russian GRU operation (as claimed by Mueller), why was the cyber spy tradecraft so sloppy? A covert cyber operation is no different from a conventional human covert operation, which means the first and guiding principle is to not leave any fingerprints that would point to the origin of the operation. In other words, you do not mistakenly leave flagrant Russian fingerprints in the document text or metadata. A good cyber spy also will not use computers and servers based in the United States and then claim it is the work of a hacker operating in Romania.

None of the Russians indicted by Mueller in his case stand accused of doing the Russian hacking while physically in the United States. No intelligence or evidence has been cited to indicate that the Russians stole a U.S. Government computer or used a GSA supplied copy of Microsoft Word to produce the G2 documents.

The name of Warren Flood, an Obama Democrat activist and Joe Biden's former Director of Information Technology, appears in at least three iterations of these documents. Did he actually masquerade as Quodlibet 2.0? If so, did he do it on his own or was he hired by someone else? These remain open questions that deserve to be investigated by John Durham, the prosecutor investigating the attempted coup against Donald Trump, and/or relevant committees of the Congress.

There are other critical unanswered questions. Obama's Attorney General, Eric Holder, sent a letter to Comey on July 26, 2016 about the the DNC hack. Lynch wrote concerning press reports that Russia attacked the DNC:

If foreign intelligence agencies are attempting to undermine that process, the U.S. government should treat such efforts even more seriously than standard espionage. These types of cyberattacks are significant and pernicious crimes. Our government must do all that it can to stop such attacks and to seek justice for the attacks that have already occurred.

We are writing to request more information on this cyberattack in particular and more information in general on how the Justice Department, FBI, and NCIJTF attempt to prevent and punish these types of cyberattacks. Accordingly, please respond to the following by August 9, 2016:

When did the Department of Justice, FBI, and NCIJTF first learn of the DNC hack? Was the government aware of the intrusion prior to the media reporting it?

Has the FBI deployed its Cyber Action Team to determine who hacked the DNC?

Has the FBI determined whether the Russian government, or any other foreign government, was involved in the hack?

In general, what actions, if any, do the Justice Department, FBI, and NCIJTF take to prevent cyberattacks on non-governmental political organizations in the U.S., such as campaigns and political parties? Does the government consult or otherwise communicate with the organizations to inform them of potential threats, relay best practices, or inform them of detected cyber intrusions?

Does the Justice Department believe that existing statutes provide an adequate basis for addressing hacking crimes of this nature, in which foreign governments hack seemingly in order to affect our electoral processes?

So far no document from Comey to Lynch has been made available to the public detailing the FBI's response to Lynch's questions. Why was the Cyber Action Team not deployed to determine who hacked the DNC? A post-mortem investigation of the DNC hack leak should have included interviews with all DNC staff, John Podesta, Warren Flood and Ethan Berkowitz. The Washington Post reporter who broke the story of the DNC hack, based on what is now in the public record, the FBI failed to do a proper investigation.

